Final Project SIEM & SOC Part 2 Michał Botuliński

Malware Analysis Report: "Dog.jpg"

Analysis Date: 15.08.2023

Report Author: Michał Botuliński

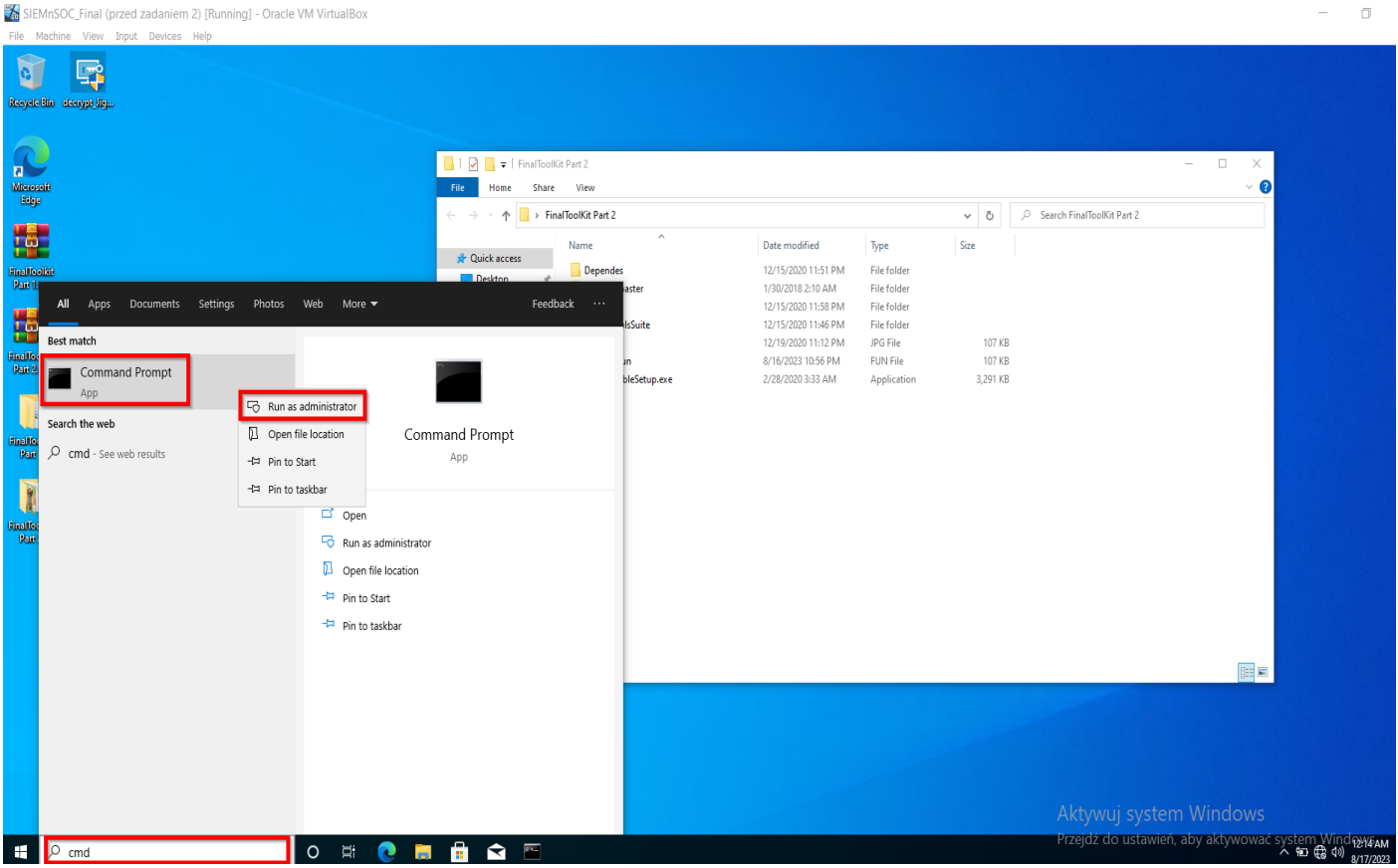
Introduction

This report documents the results of the analysis of the "Dog.jpg" file in the context of detecting potential presence of malicious software (malware). The first part of the analysis focused on identifying potentially suspicious strings within the file using the strings64.exe tool from the SysInternals suite.

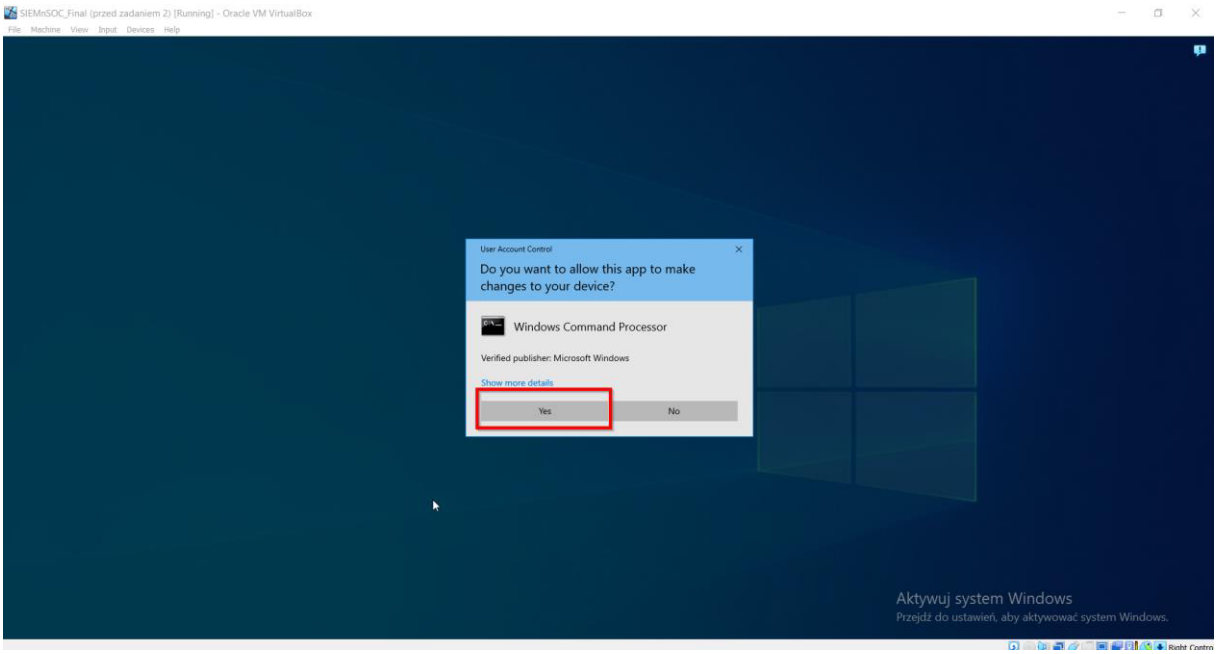
2. Analysis Tool – strings64.exe

The analysis of the "Dog.jpg" file utilized the strings64.exe tool from the SysInternals suite. This tool enables the extraction of textual characters from binary files, which can reveal hidden or encoded information.

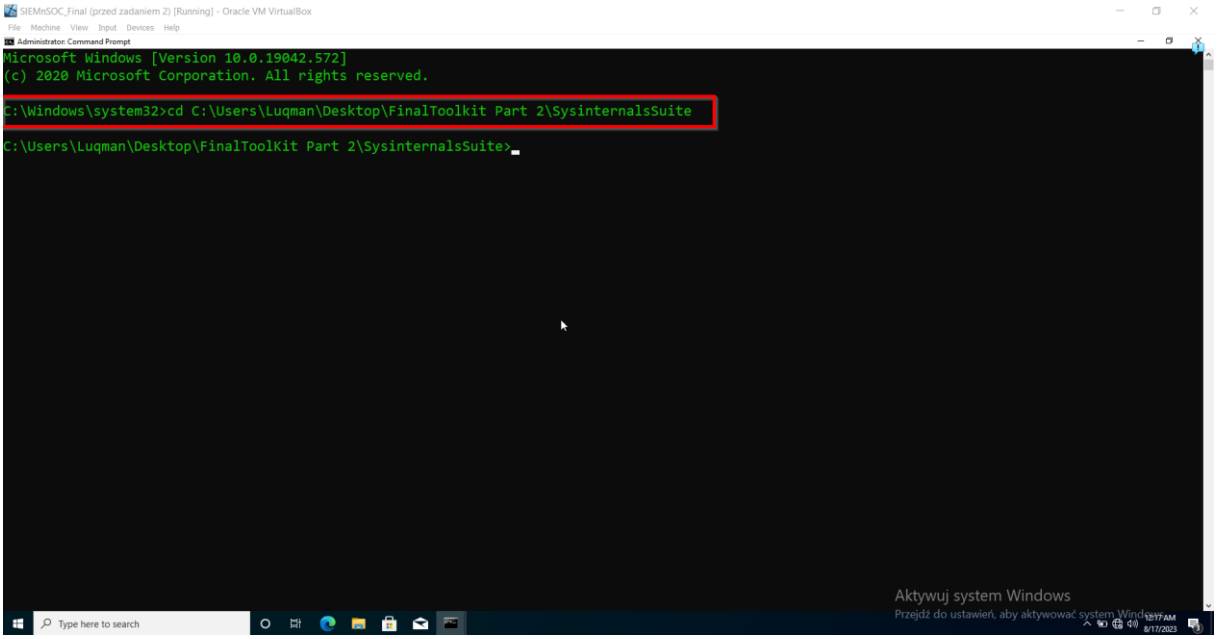
a)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
decrypt_lig...
Microsoft Edge
FinalToolkit Part 1
FinalToolKit Part 2
File Home Share View
Search FinalToolKit Part 2
Quick access
Name
Date modified
Type
Size
All Apps Documents Settings Photos Web More
Feedback
Best match
Command Prompt
App
Search the web
cmd - See web results
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
cmd
Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows.

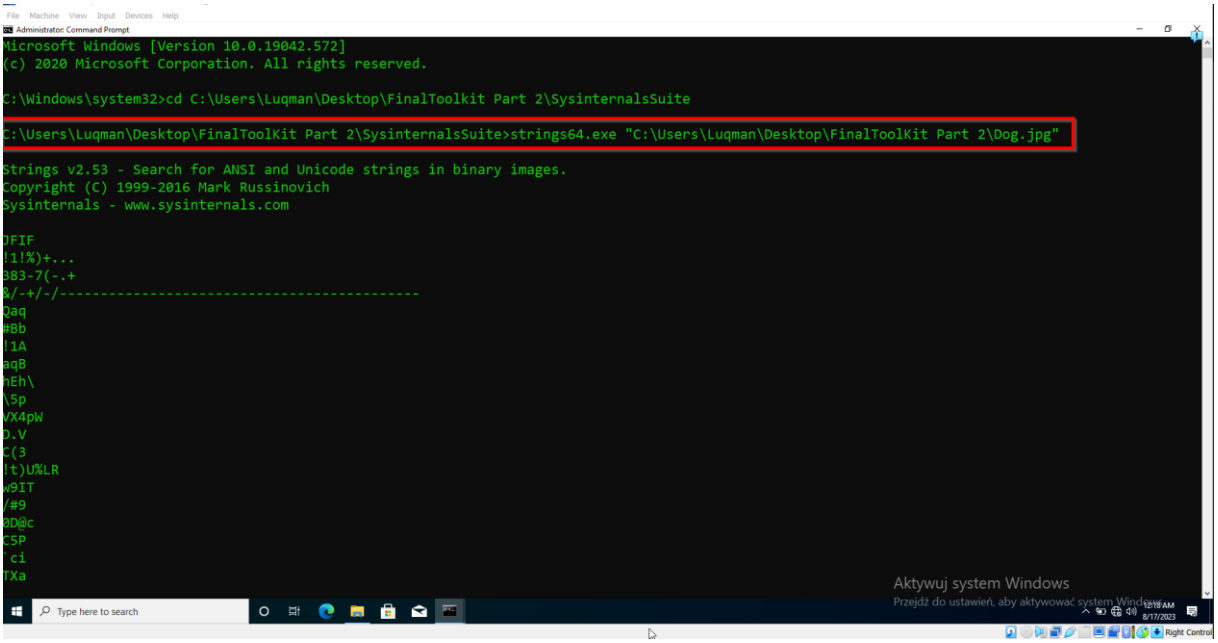
b)


User Account Control
Do you want to allow this app to make changes to your device?
Windows Command Processor
Verified publisher: Microsoft Windows
Show more details
Yes
No
Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows.

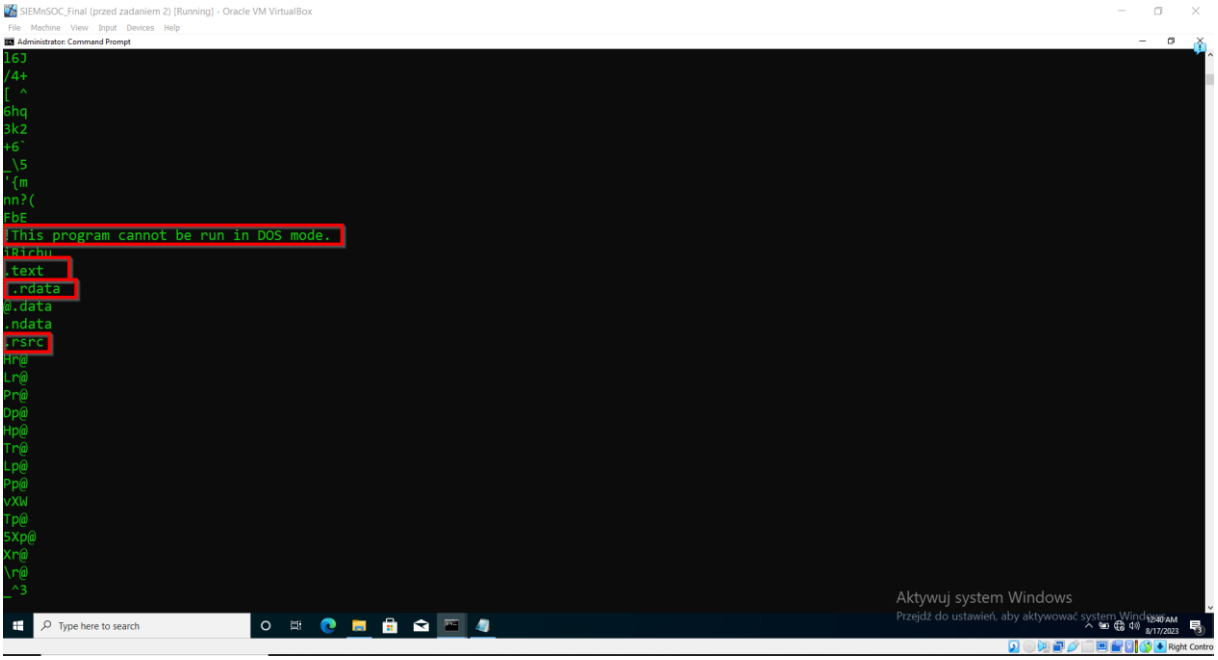
c)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.572]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd C:\Users\Luqman\Desktop\FinalToolkit Part 2\SysinternalsSuite
C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite>
Type here to search
Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows.
8/17/2023

d)


File Machine View Input Devices Help
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.572]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd C:\Users\Luqman\Desktop\FinalToolkit Part 2\SysinternalsSuite
C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite>strings64.exe "C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg"
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
JFIF
!1!%)+...
383-7(-.+
%/-+/-/----------
Qaq
#Bb
!1A
aqB
hEh\
\5p
VX4pW
D.V
C(3
!t)U%LR
w9IT
/#9
0D@c
C5P
ci
TXa
Type here to search
Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows.
8/17/2023
Right Control

e)



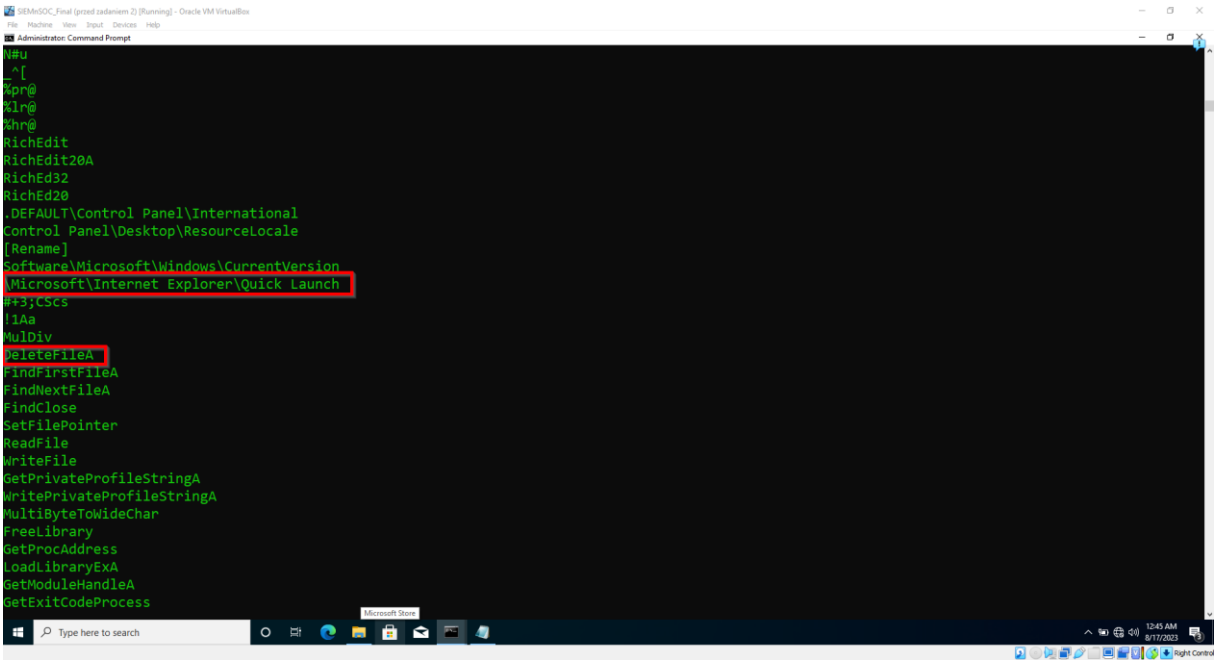
- **!This program cannot be run in Dos mode** is a characteristic message that often appears in executable files of programs for Windows systems.

- **.text** This Section generally contains the CPU instructions executed when the PE file is run. This section is marked as executable.

- **.rdata** typically refers to all kinds of constant textual information used by the program, such as user messages, filenames, function names, constant configurations, etc.

- **.rsrc** This Section contains resources that are used by the PE file, for example, images, icons, etc.

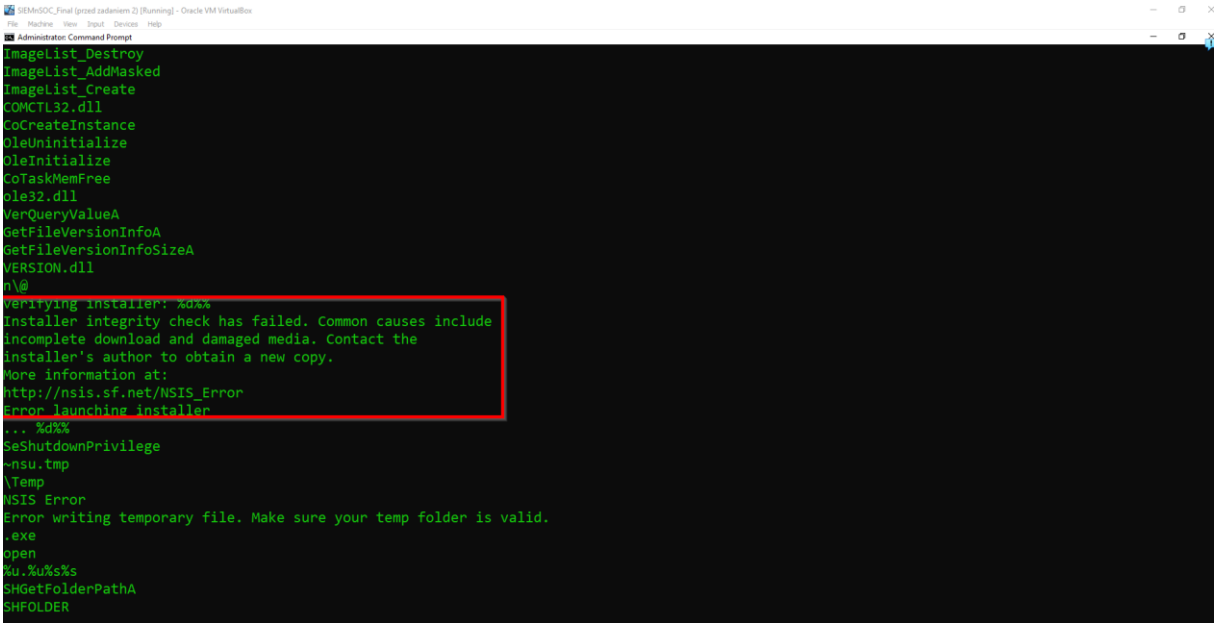
f)



- ***\Microsoft\Internet Explorer\Quick Launch:*** This refers to a location in the registry or file system that could contain shortcuts to frequently visited websites in the "Quick Launch" menu of the Internet Explorer browser (an older Microsoft browser) or in later versions of Windows, in the "Quick Launch" area of the taskbar.

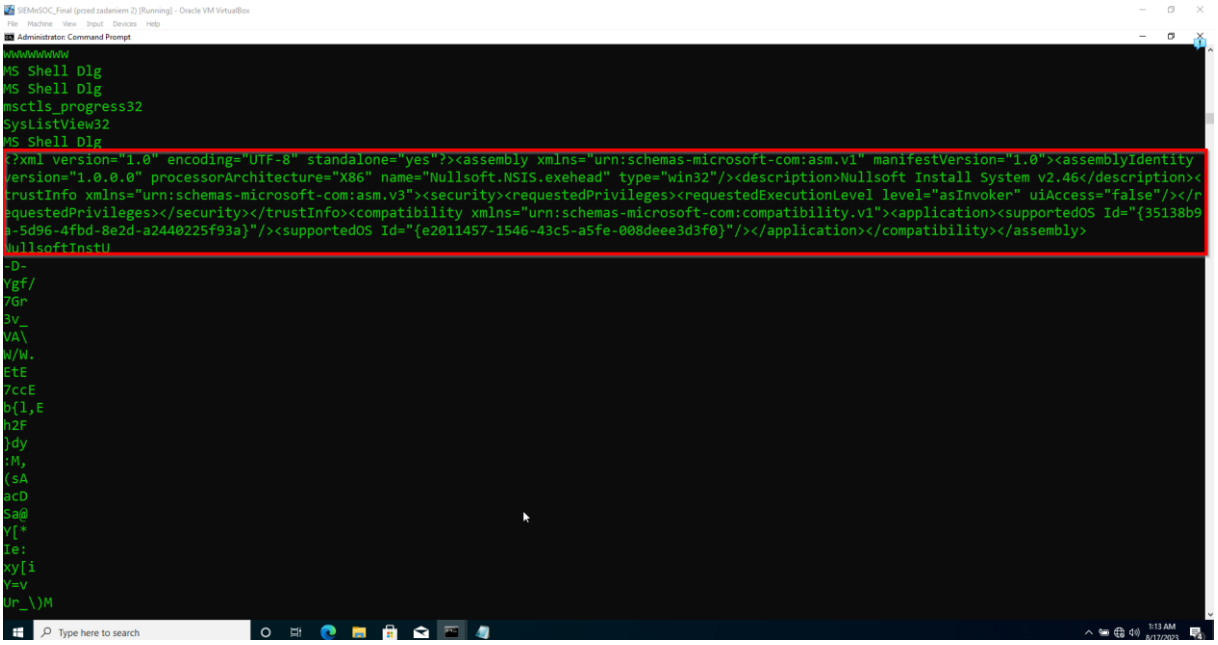
- The **"DeleteFileA"** function is used to delete a file from the file system. It's a part of the Windows API and provides a way for programs to interact with the file system to perform various file-related operations, such as creating, opening, reading, writing, and deleting files.

g)



- **string verifying installer: %d%% Installer integrity check has failed. Common causes include incomplete download and damaged media. Contact the installer's author to obtain a new copy. More information at: http://nsis.sf.net/NSIS_Error Error launching installer** - text seems to be an error message related to an installer.

h)

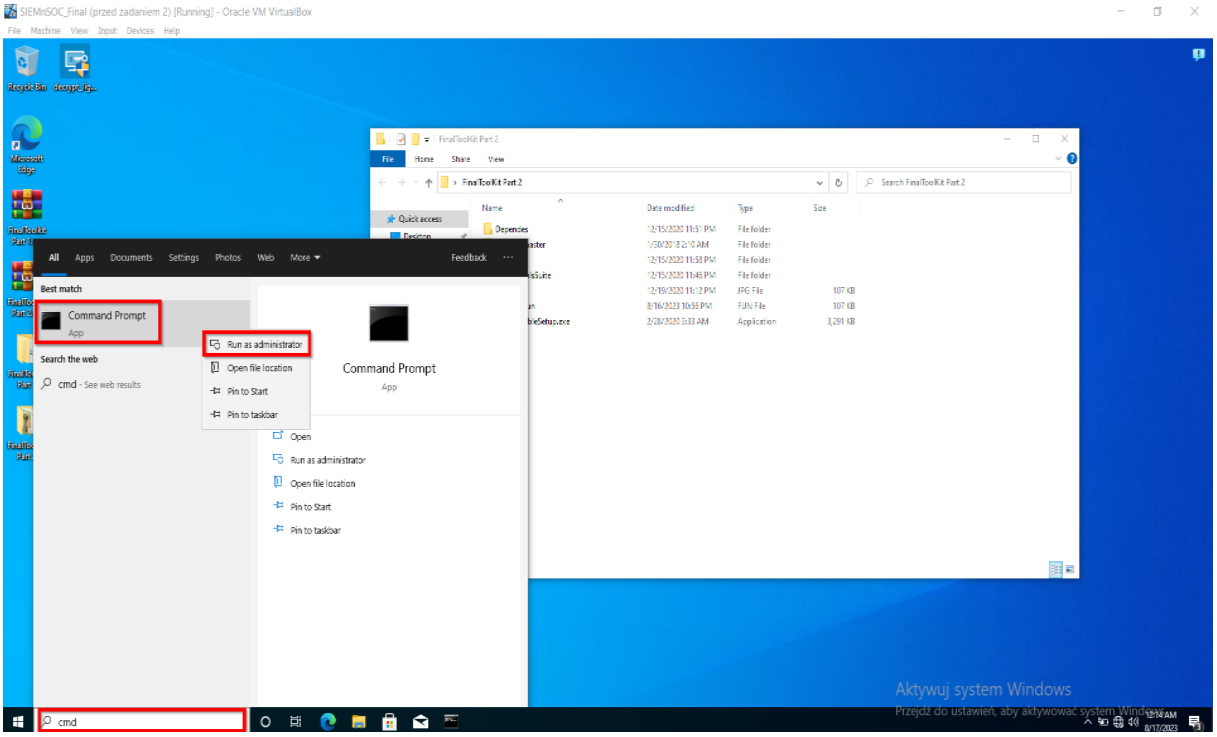


- **<?xml version="1.0" encoding="UTF-8" standalone="yes"?><assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0"><assemblyIdentity version="1.0.0.0" processorArchitecture="X86" name="Nullsoft.NSIS.exehead" type="win32"/><description>Nullsoft Install System v2.46</description><trustInfo xmlns="urn:schemas-microsoft-com:asm.v3"><security><requestedPrivileges><requestedExecutionLevel level="asInvoker" uiAccess="false"/></requestedPrivileges></security></trustInfo><compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1"><application><supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/><supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"/></application></compatibility></assembly>** - The entire XML fragment constitutes the manifest of an application or installer created using NSIS (Nullsoft Scriptable Install System). This manifest contains information about the application, its requirements, and compatibility with the operating system.

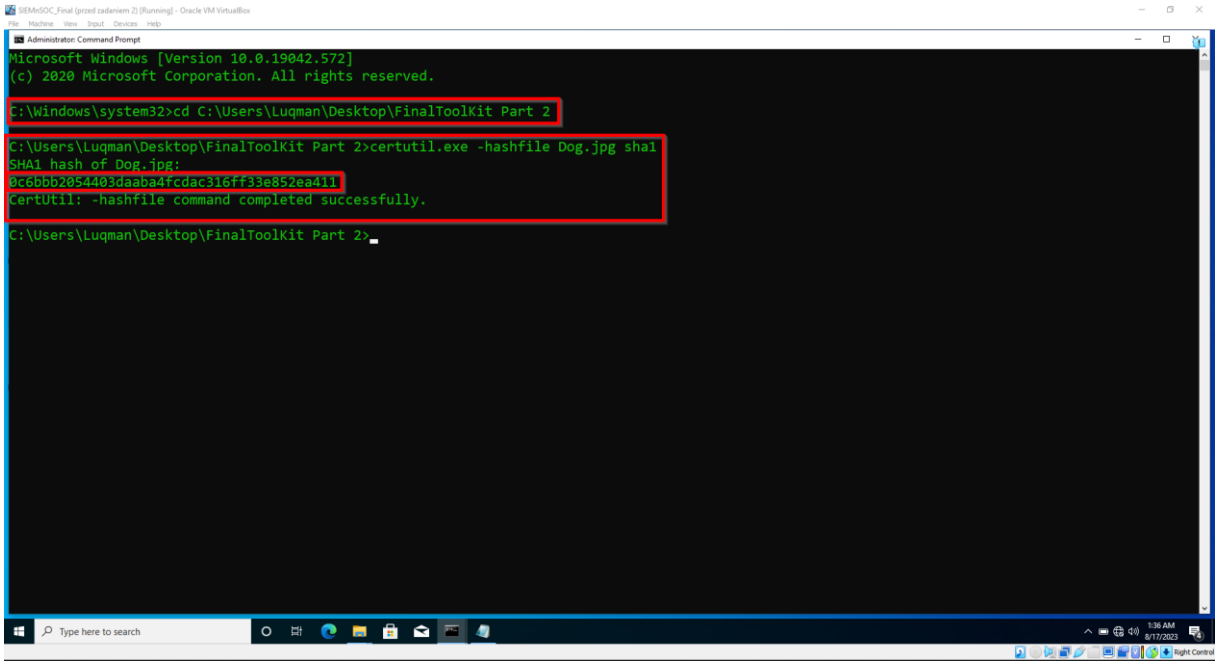
2.Hash Extraction and VirusTotal Analysis

The SHA-1 hash of the "Dog.jpg" file was extracted using the certutil.exe tool. This hash was then submitted to the www.virustotal.com online platform for analysis. The results of this analysis revealed that the file in question is indeed recognized as malicious by various antivirus engines present on the VirusTotal platform. Also further analysis was conducted on the VirusTotal platform, specifically in the "Graph Summary" tab, which led to the remarkable discovery of a hidden "exe" file embedded within the binary data of "Dog.jpg." This revelation underscores the elevated complexity of the threat, suggesting the utilization of advanced techniques such as steganography or encryption.

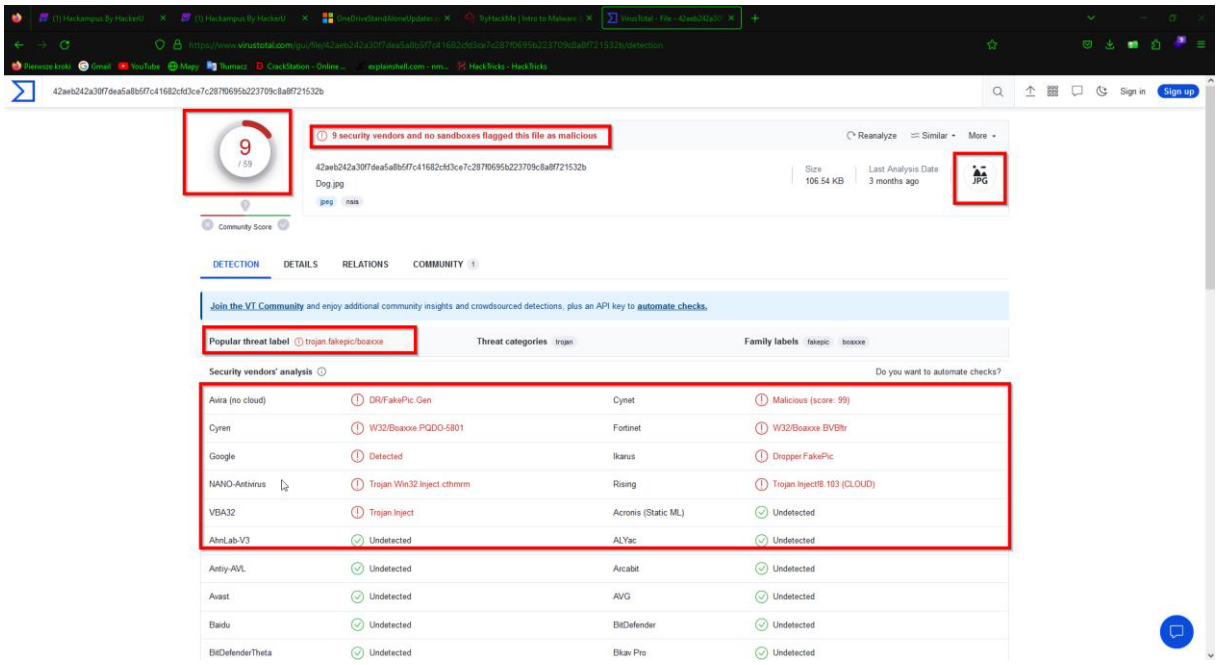
a)



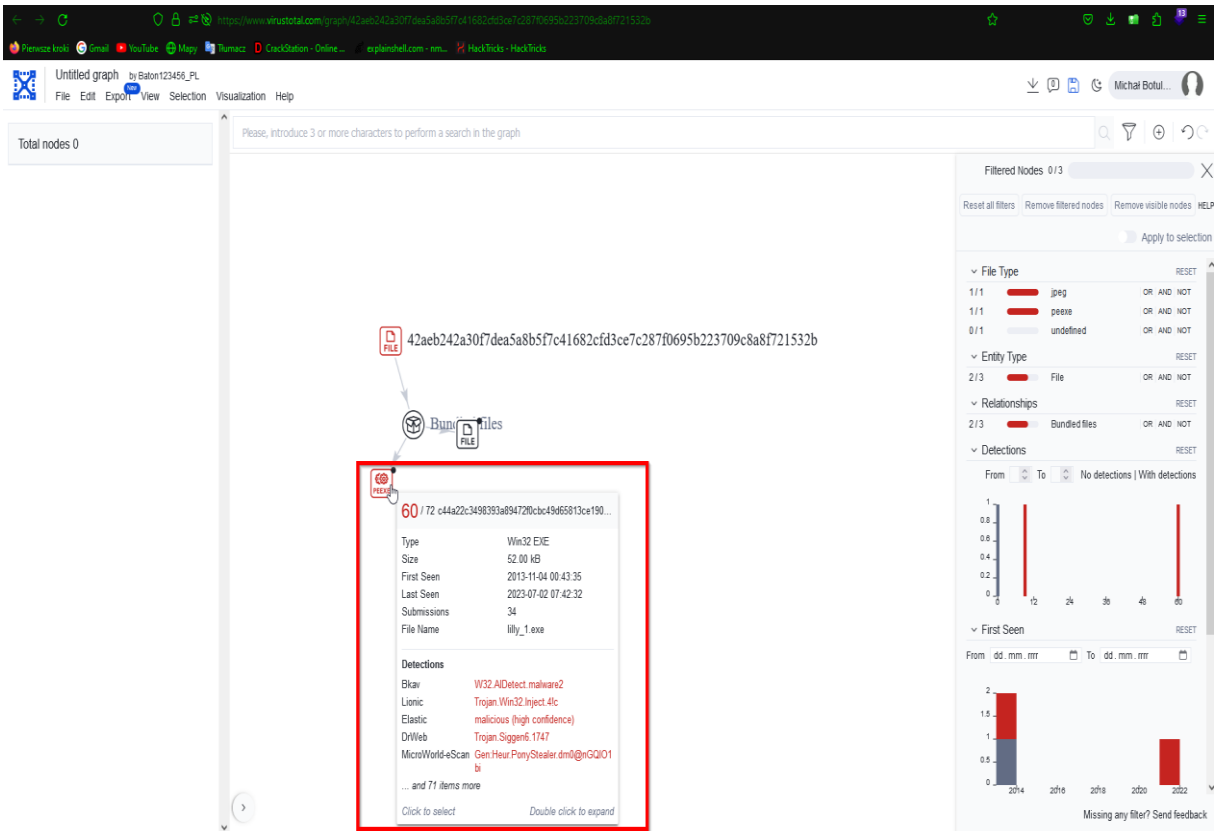
b)


Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.572]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd C:\Users\Luqman\Desktop\FinalToolKit Part 2
C:\Users\Luqman\Desktop\FinalToolKit Part 2>certutil.exe -hashfile Dog.jpg sha1
SHA1 hash of Dog.jpg:
0c6bbb2054403daaba4fcdac316ff33e852ea411
CertUtil: -hashfile command completed successfully.
C:\Users\Luqman\Desktop\FinalToolKit Part 2>
Type here to search

c)


42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c8a8f721532b
9 / 59
9 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c8a8f721532b
Dog.jpg
Size
106.54 KB
Last Analysis Date
3 months ago
JPG
Community Score
DETECTION
DETAILS
RELATIONS
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.fakepic/boaxxe
Threat categories trojan
Family labels fakepic boaxxe
Security vendors' analysis
Do you want to automate checks?
Avira (no cloud) DR/FakePic.Gen
Cynet Malicious (score: 99)
Cyren W32/Boaxxe.PQDO-5801
Fortinet W32/Boaxxe.BVBltr
Google Detected
Ikarus Dropper.FakePic
NANO-Antivirus Trojan.Win32.Inject.cthmrm
Rising Trojan.Inject!8.103 (CLOUD)
VBA32 Trojan.Inject
Acronis (Static ML) Undetected
AhnLab-V3 Undetected
ALYac Undetected
Antiy-AVL Undetected
Arcabit Undetected
Avast Undetected
AVG Undetected
Baidu Undetected
BitDefender Undetected
BitDefenderTheta Undetected
Bkav Pro Undetected

d)

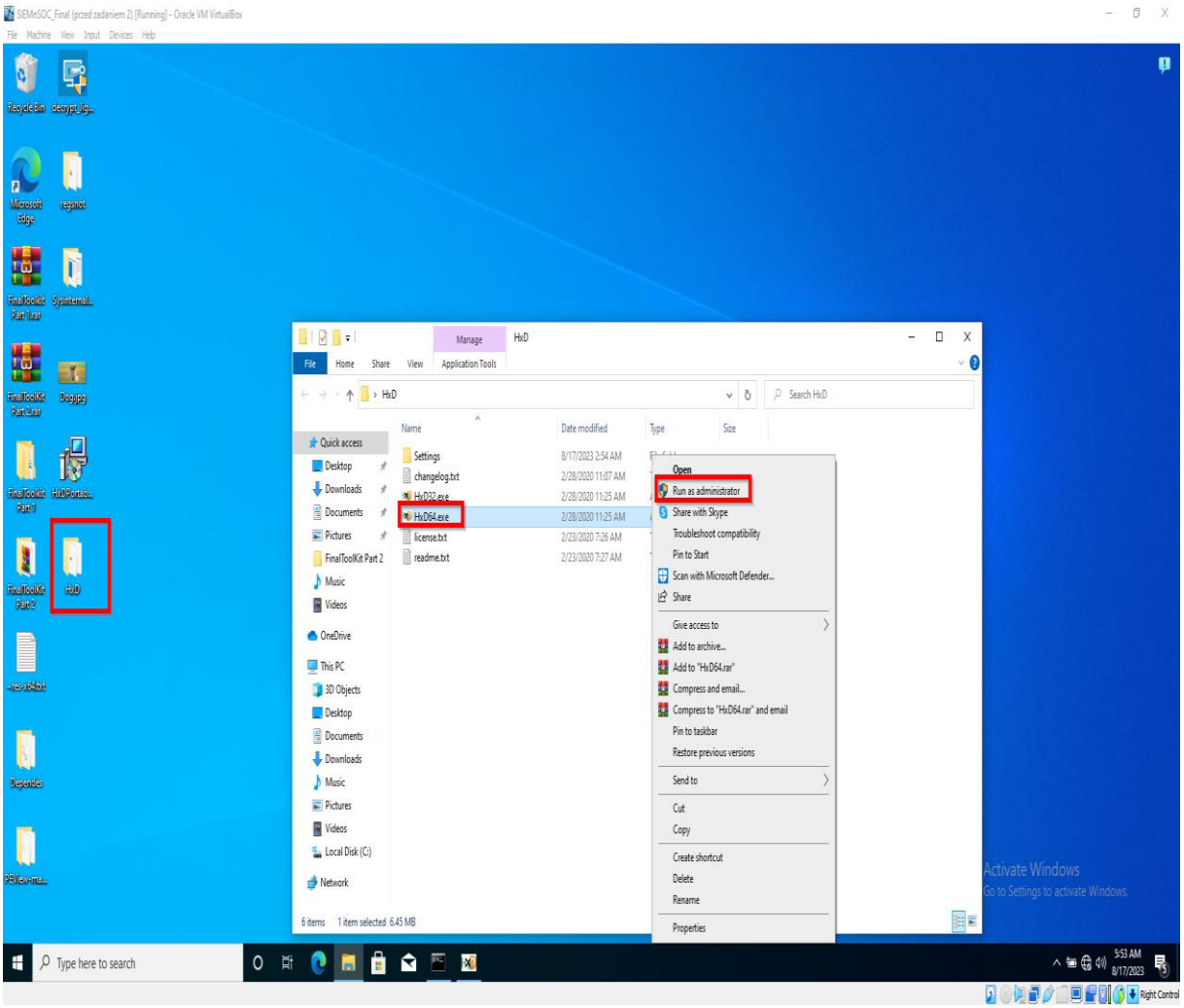

Untitled graph
by Baton123456_PL
File Edit Export View Selection Visualization Help
Total nodes 0
Please, introduce 3 or more characters to perform a search in the graph
42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c8a8f721532b
60 / 72 c44a22c3498393a89472f0cbc49d65813ce190...
Type Win32 EXE
Size 52.00 kB
First Seen 2013-11-04 00:43:35
Last Seen 2023-07-02 07:42:32
Submissions 34
File Name lilly_1.exe
Detections
Bkav W32.AIDetect.malware2
Lionic Trojan.Win32.Inject.4!c
Elastic malicious (high confidence)
DrWeb Trojan.Siggen6.1747
MicroWorld-eScan Gen:Heur.PonyStealer.dm0@nGQlO1bi
... and 71 items more
Click to select
Double click to expand
Filtered Nodes 0 / 3
Reset all filters
Remove filtered nodes
Remove visible nodes
Apply to selection
File Type
Entity Type
Relationships
Bundled files
Detections
No detections | With detections
First Seen
Missing any filter? Send feedback

3. In this section of report the findings of the malware file analysis, with a specific focus on the process of extracting a hidden "exe" file from the "Dog.jpg" file. The analysis also encompasses the identification of missing DLL libraries required by the program and aspects related to the detectability of the extracted "exe" file.

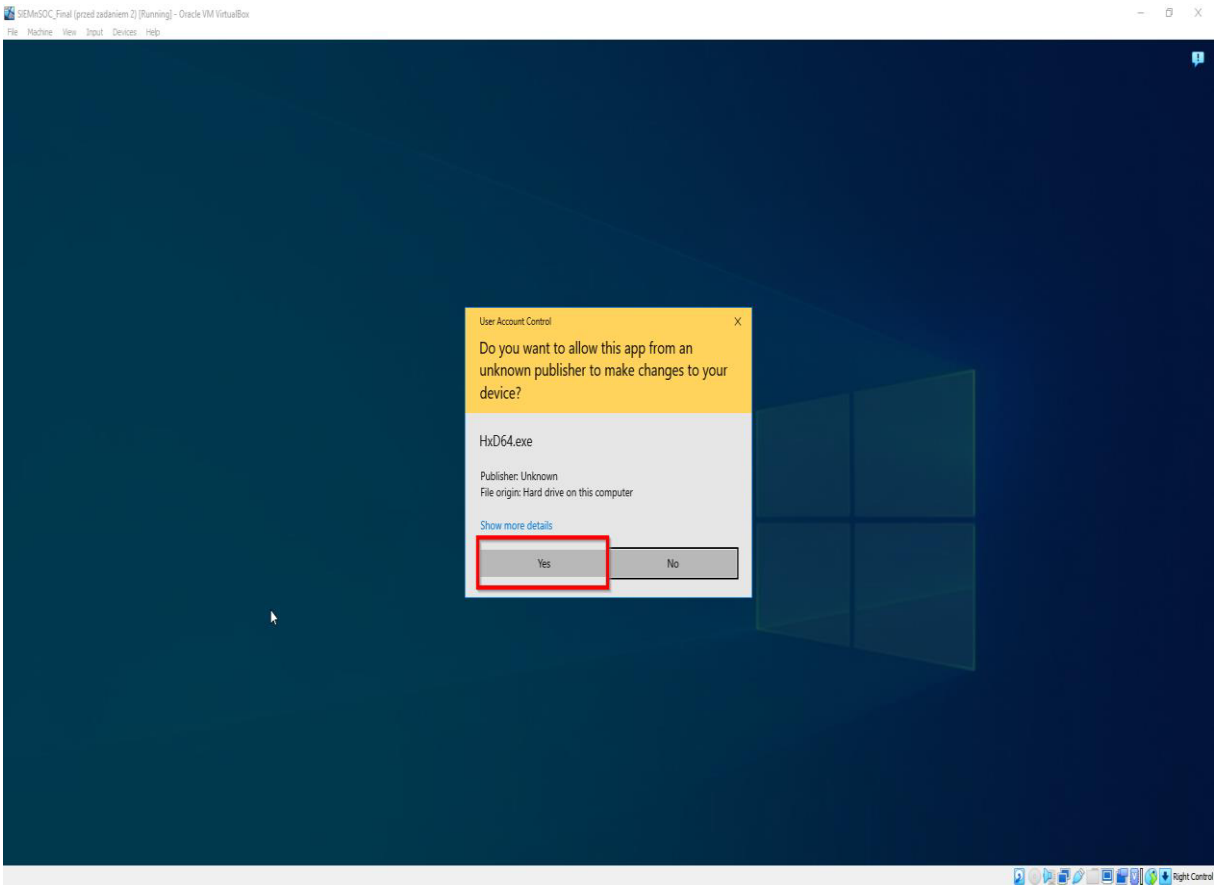
The analysis of the malware file commenced with the extraction process of the concealed "exe" file by use “HxD” program. This procedure aimed at revealing the content of this file and comprehending its functionality. The initial step involved locating the beginning of the program, which was covertly embedded within the "Dog.jpg" file. Upon discovering the "4D 5A" sequence (MZ header), the endeavor to copy the entire line from this sequence to the end of the file was undertaken. Subsequently, the duplicated sequence was stored as a novel file named "untitled.exe."

Post preparation of the "untitled.exe" file, a thorough analysis was executed employing the Dependency Walker tool. This initiative was aimed at identifying the DLL libraries indispensable for the program's seamless functioning.

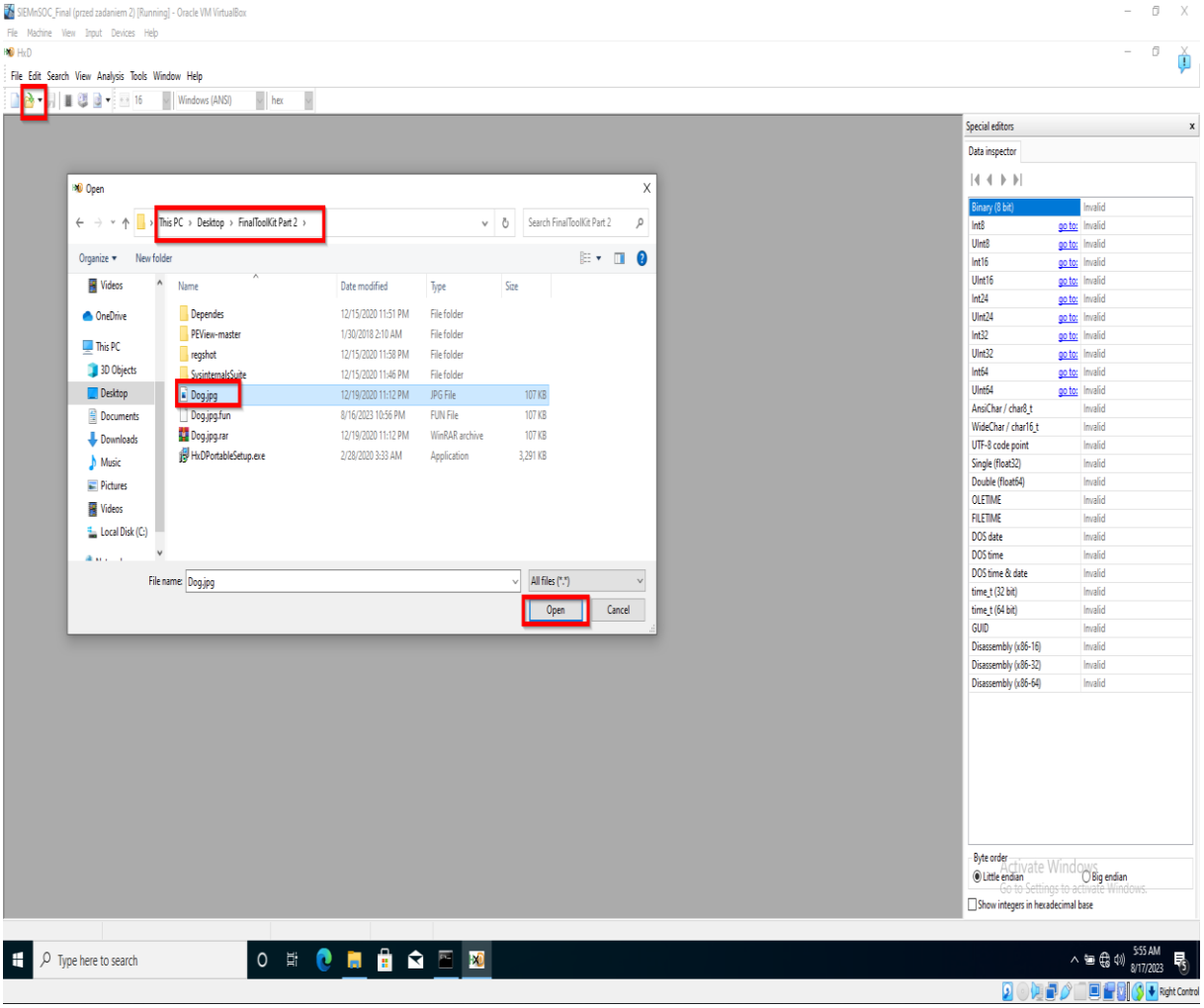
One of DLL’s found via Dependency walker that program uses, which is not found is **API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL**.



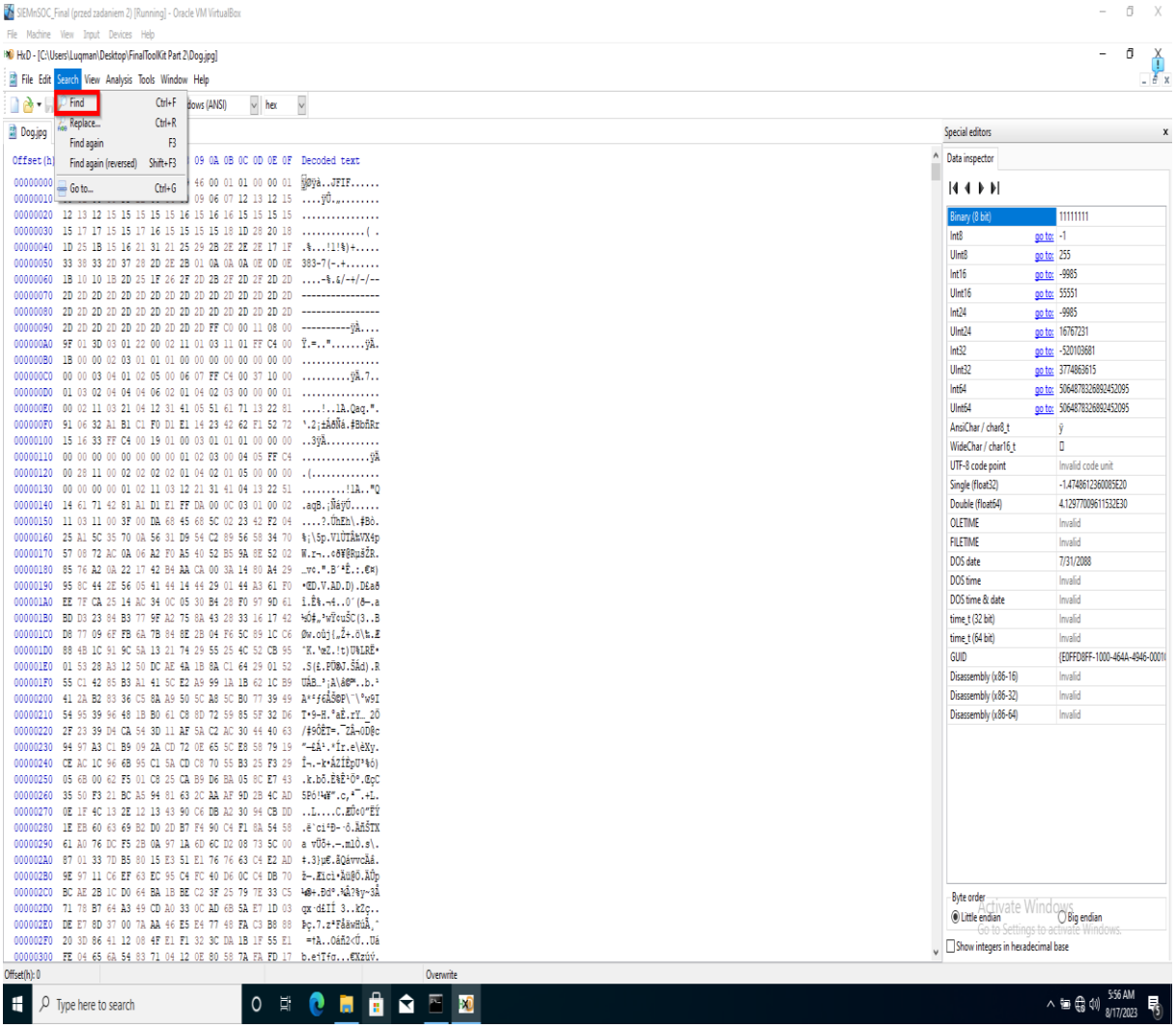
b)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
User Account Control
Do you want to allow this app from an unknown publisher to make changes to your device?
HxD64.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show more details
Yes
No
Right Control

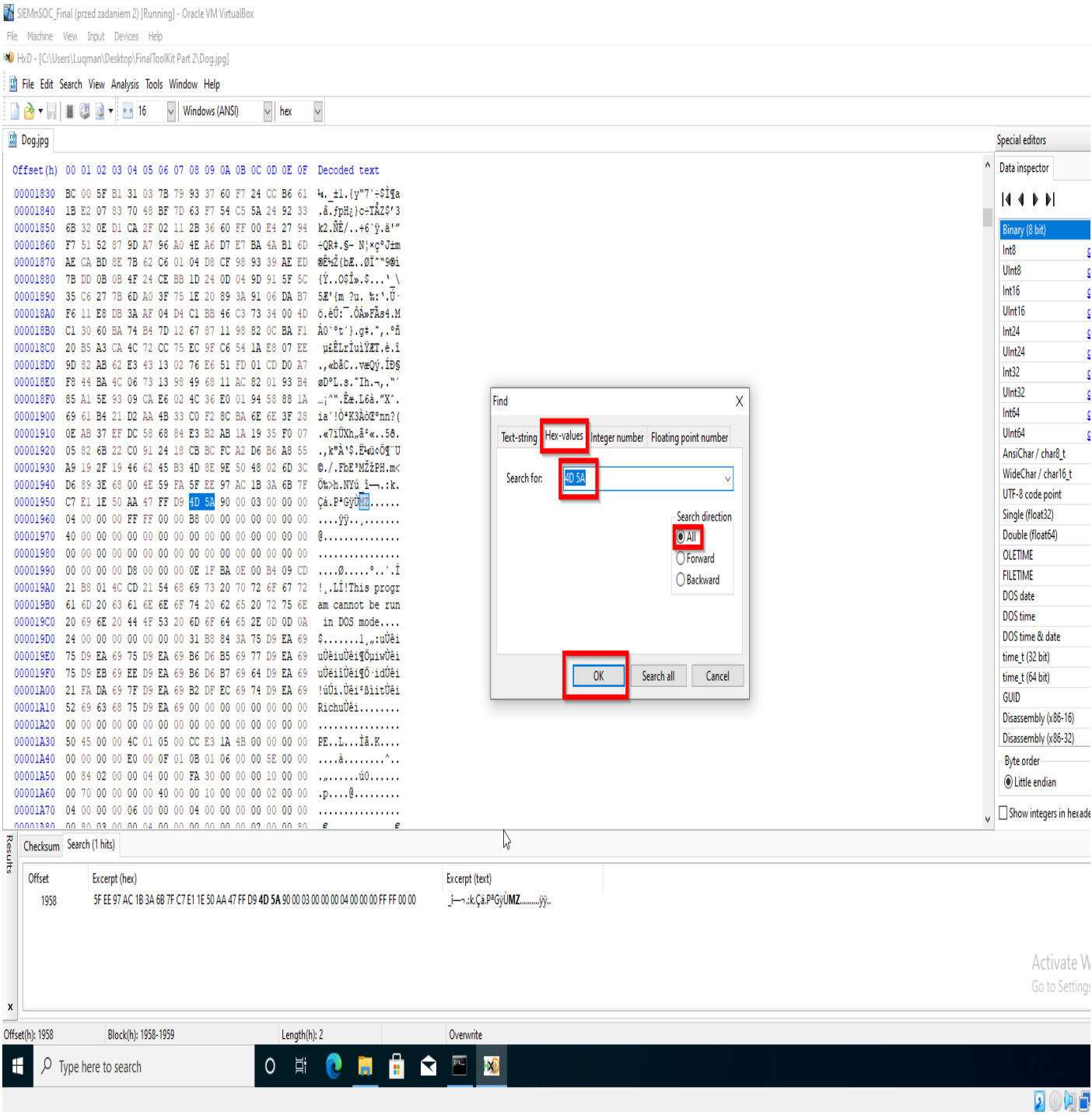
c)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HxD
File Edit Search View Analysis Tools Window Help
Open
This PC › Desktop › FinalToolKit Part 2 ›
Search FinalToolKit Part 2
Organize
New folder
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Date modified
Type
Size
Dependes
PEView-master
regshot
SysinternalsSuite
Dog.jpg
Dog.jpg.fun
Dog.jpg.rar
HxDPortableSetup.exe
File name: Dog.jpg
All files (*.*)
Open
Cancel
Special editors
Data inspector
Byte order
Little endian
Big endian
Show integers in hexadecimal base
Activate Windows
Type here to search
5:55 AM
8/17/2023
Right Control

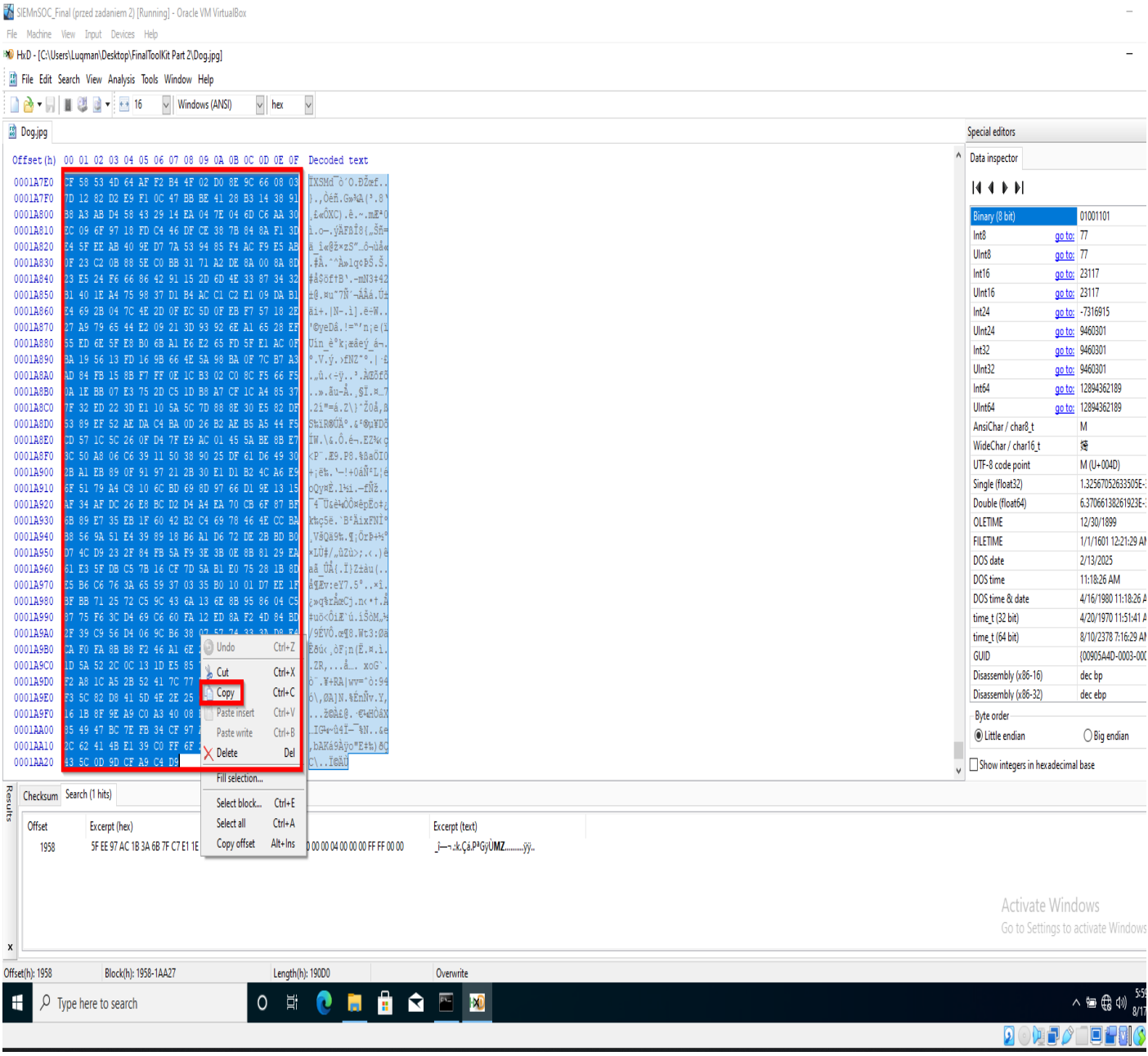
d)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HxD - [C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg]
File Edit Search View Analysis Tools Window Help
Find Ctrl+F
Replace... Ctrl+R
Find again F3
Find again (reversed) Shift+F3
Go to... Ctrl+G
Dog.jpg
Special editors
Data inspector
Byte order
Little endian
Big endian
Show integers in hexadecimal base
Activate Windows
Go to Settings to activate Windows.
Offset(h): 0
Overwrite
Type here to search
5:56 AM
8/17/2023

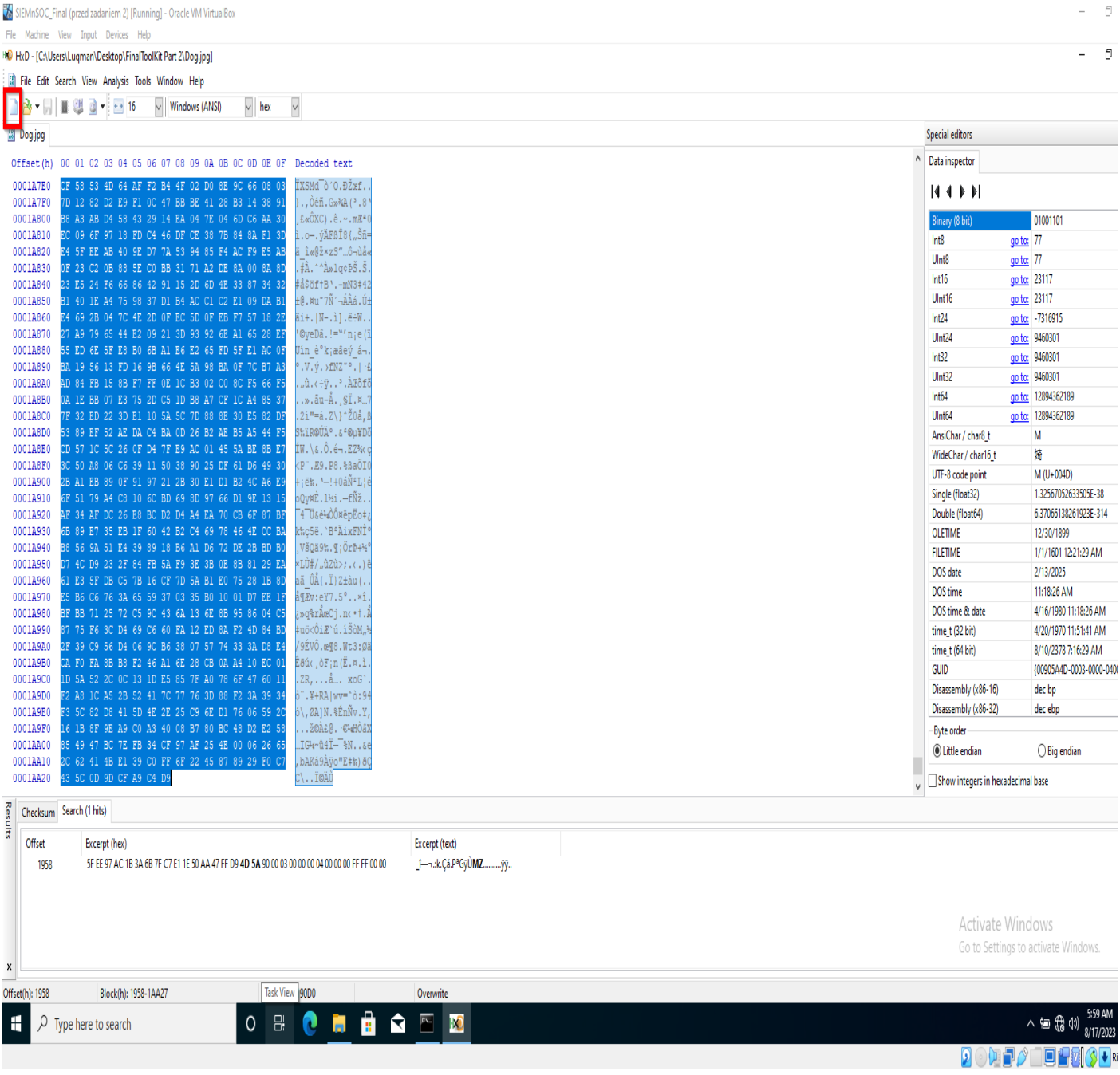
e)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HxD - [C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg]
File Edit Search View Analysis Tools Window Help
Windows (ANSI)
hex
Dog.jpg
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00001830 BC 00 5F B1 31 03 7B 79 93 37 60 F7 24 CC B6 61
00001840 1B E2 07 83 70 48 BF 7D 63 F7 54 C5 5A 24 92 33
00001850 6B 32 0E D1 CA 2F 02 11 2B 36 60 FF 00 E4 27 94
00001860 F7 51 52 87 9D A7 96 A0 4E A6 D7 E7 BA 4A B1 6D
00001870 AE CA BD 8E 7B 62 C6 01 04 D8 CF 98 93 39 AE ED
00001880 7B DD 0B 0B 4F 24 CE BB 1D 24 0D 04 9D 91 5F 5C
00001890 35 C6 27 7B 6D A0 3F 75 1E 20 89 3A 91 06 DA B7
000018A0 F6 11 E8 DB 3A AF 04 D4 C1 BB 46 C3 73 34 00 4D
000018B0 C1 30 60 BA 74 B4 7D 12 67 87 11 98 82 0C BA F1
000018C0 20 B5 A3 CA 4C 72 CC 75 EC 9F C6 54 1A E8 07 EE
000018D0 9D 82 AB 62 E3 43 13 02 76 E6 51 FD 01 CD D0 A7
000018E0 F8 44 BA 4C 06 73 13 98 49 68 11 AC 82 01 93 B4
000018F0 85 A1 5E 93 09 CA E6 02 4C 36 E0 01 94 58 88 1A
00001900 69 61 B4 21 D2 AA 4B 33 C0 F2 8C BA 6E 6E 3F 28
00001910 0E AB 37 EF DC 58 68 84 E3 B2 AB 1A 19 35 F0 07
00001920 05 82 6B 22 C0 91 24 18 CB BC FC A2 D6 B6 A8 55
00001930 A9 19 2F 19 46 62 45 B3 4D 8E 50 48 02 6D 3C
00001940 D6 89 3E 68 00 4E 59 FA 5F EE 97 AC 1B 3A 6B 7F
00001950 C7 E1 1E 50 AA 47 FF D9 4D 5A 90 00 03 00 00 00
00001960 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00
00001970 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001980 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001990 00 00 00 00 D8 00 00 00 0E 1F BA 0E 00 B4 09 CD
000019A0 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72
000019B0 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E
000019C0 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A
000019D0 24 00 00 00 00 00 00 00 31 B8 84 3A 75 D9 EA 69
000019E0 75 D9 EA 69 75 D9 EA 69 B6 D6 B5 69 77 D9 EA 69
000019F0 75 D9 EB 69 EE D9 EA 69 B6 D6 B7 69 64 D9 EA 69
00001A00 21 FA DA 69 7F D9 EA 69 B2 DF EC 69 74 D9 EA 69
00001A10 52 69 63 68 75 D9 EA 69 00 00 00 00 00 00 00 00
00001A20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001A30 50 45 00 00 4C 01 05 00 CC E3 1A 4B 00 00 00 00
00001A40 00 00 00 00 E0 00 0F 01 0B 01 06 00 00 5E 00 00
00001A50 00 84 02 00 00 04 00 00 FA 30 00 00 00 10 00 00
00001A60 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00
00001A70 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00
Special editors
Data inspector
Binary (8 bit)
Int8
UInt8
Int16
UInt16
Int24
UInt24
Int32
UInt32
Int64
UInt64
AnsiChar / char8_t
WideChar / char16_t
UTF-8 code point
Single (float32)
Double (float64)
OLETIME
FILETIME
DOS date
DOS time
DOS time & date
time_t (32 bit)
time_t (64 bit)
GUID
Disassembly (x86-16)
Disassembly (x86-32)
Byte order
Little endian
Show integers in hexade
Find
Text-string
Hex-values
Integer number
Floating point number
Search for:
4D 5A
Search direction
All
Forward
Backward
OK
Search all
Cancel
Results
Checksum
Search (1 hits)
Offset
Excerpt (hex)
Excerpt (text)
1958
5F EE 97 AC 1B 3A 6B 7F C7 E1 1E 50 AA 47 FF D9 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
Offset(h): 1958
Block(h): 1958-1959
Length(h): 2
Overwrite
Type here to search

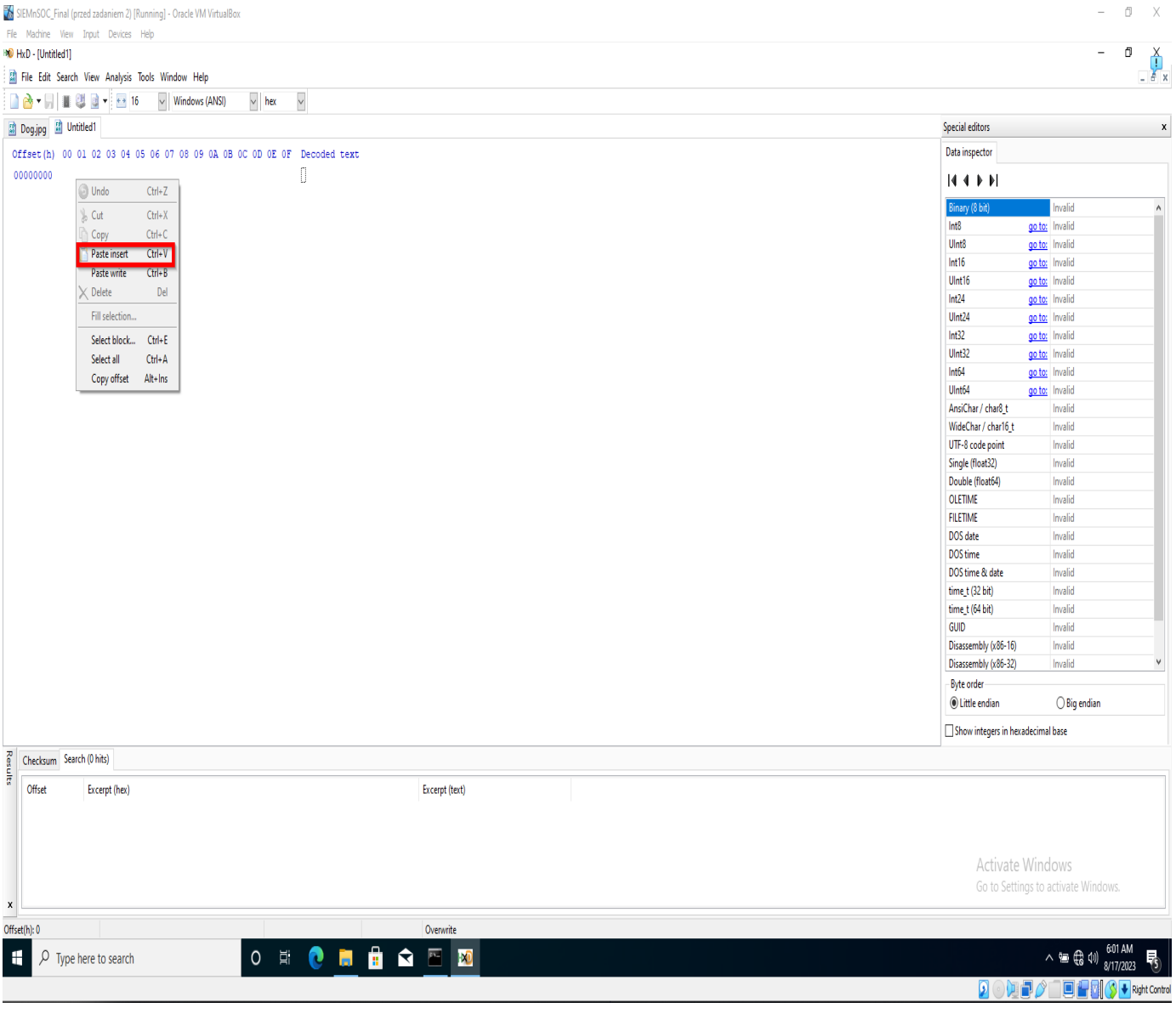
f)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HxD - [C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg]
File Edit Search View Analysis Tools Window Help
Dog.jpg
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
Undo Ctrl+Z
Cut Ctrl+X
Copy Ctrl+C
Paste insert Ctrl+V
Paste write Ctrl+B
Delete Del
Fill selection...
Select block... Ctrl+E
Select all Ctrl+A
Copy offset Alt+Ins
Special editors
Data inspector
Binary (8 bit) 01001101
Int8 77
Uint8 77
Int16 23117
Uint16 23117
Int24 -7316915
Uint24 9460301
Int32 9460301
Uint32 9460301
Int64 12894362189
Uint64 12894362189
AnsiChar / char8_t M
WideChar / char16_t
UTF-8 code point M (U+004D)
Single (float32)
Double (float64)
OLETIME 12/30/1899
FILETIME 1/1/1601 12:21:29 AM
DOS date 2/13/2025
DOS time 11:18:26 AM
DOS time & date 4/16/1980 11:18:26 A
time_t (32 bit) 4/20/1970 11:51:41 A
time_t (64 bit) 8/10/2378 7:16:29 AM
GUID {00905A4D-0003-000
Disassembly (x86-16) dec bp
Disassembly (x86-32) dec ebp
Byte order
Little endian
Big endian
Show integers in hexadecimal base
Results
Checksum
Search (1 hits)
Offset
Excerpt (hex)
Excerpt (text)
1958
Activate Windows
Go to Settings to activate Windows
Offset(h): 1958
Block(h): 1958-1AA27
Length(h): 190D0
Overwrite
Type here to search

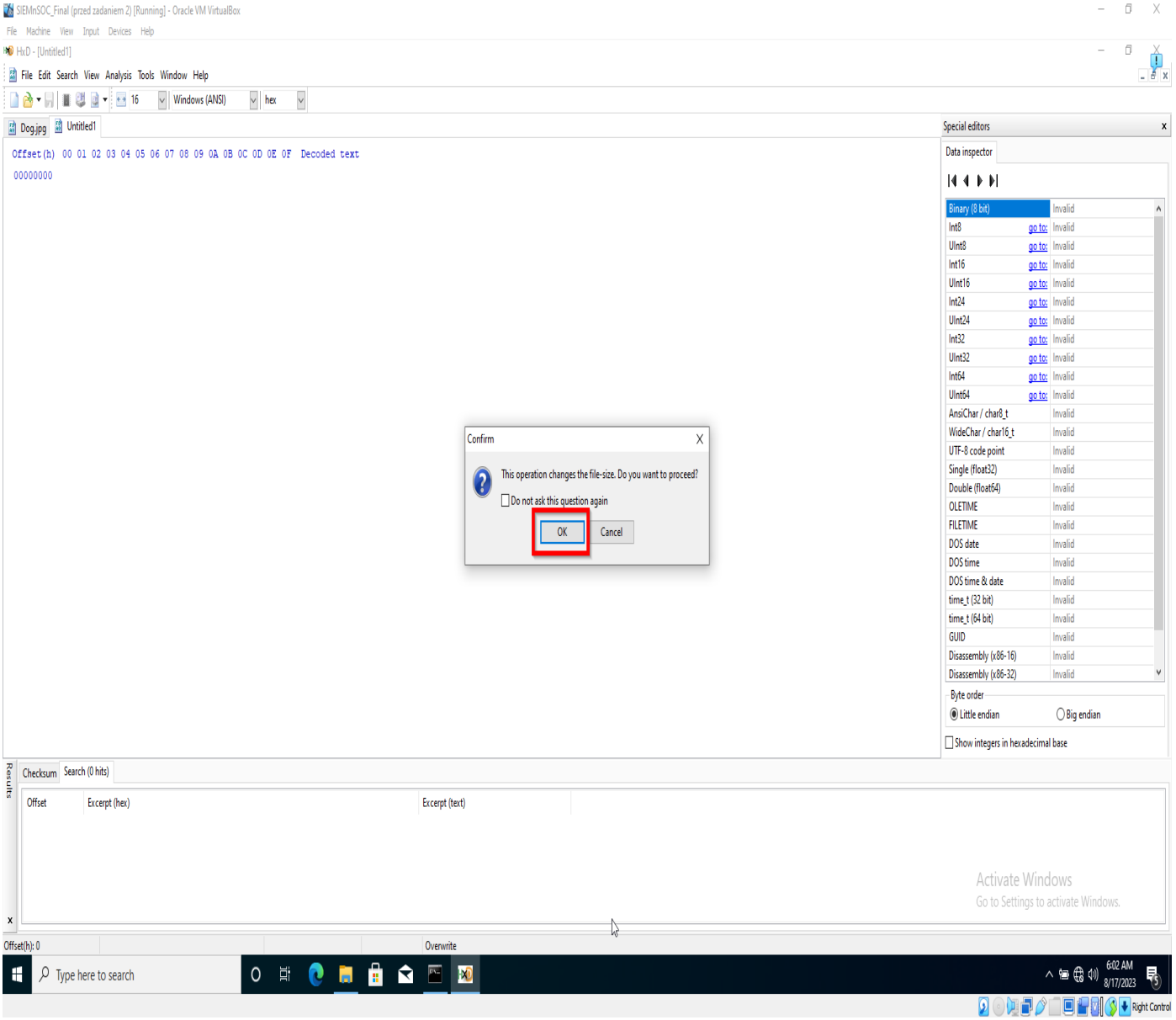
g)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HxD - [C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg]
File Edit Search View Analysis Tools Window Help
Windows (ANSI)
hex
Dog.jpg
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
Special editors
Data inspector
Binary (8 bit) 01001101
Int8 77
UInt8 77
Int16 23117
UInt16 23117
Int24 -7316915
UInt24 9460301
Int32 9460301
UInt32 9460301
Int64 12894362189
UInt64 12894362189
AnsiChar / char8_t M
WideChar / char16_t
UTF-8 code point M (U+004D)
Single (float32) 1.32567052633505E-38
Double (float64) 6.37066138261923E-314
OLETIME 12/30/1899
FILETIME 1/1/1601 12:21:29 AM
DOS date 2/13/2025
DOS time 11:18:26 AM
DOS time & date 4/16/1980 11:18:26 AM
time_t (32 bit) 4/20/1970 11:51:41 AM
time_t (64 bit) 8/10/2378 7:16:29 AM
GUID {00905A4D-0003-0000-040
Disassembly (x86-16) dec bp
Disassembly (x86-32) dec ebp
Byte order
Little endian
Big endian
Show integers in hexadecimal base
Results
Checksum
Search (1 hits)
Offset
Excerpt (hex)
Excerpt (text)
1958 5F EE 97 AC 1B 3A 6B 7F C7 E1 1E 50 AA 47 FF D9 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
Activate Windows
Go to Settings to activate Windows.
Offset(h): 1958
Block(h): 1958-1AA27
Task View
Overwrite
Type here to search
5:59 AM
8/17/2023

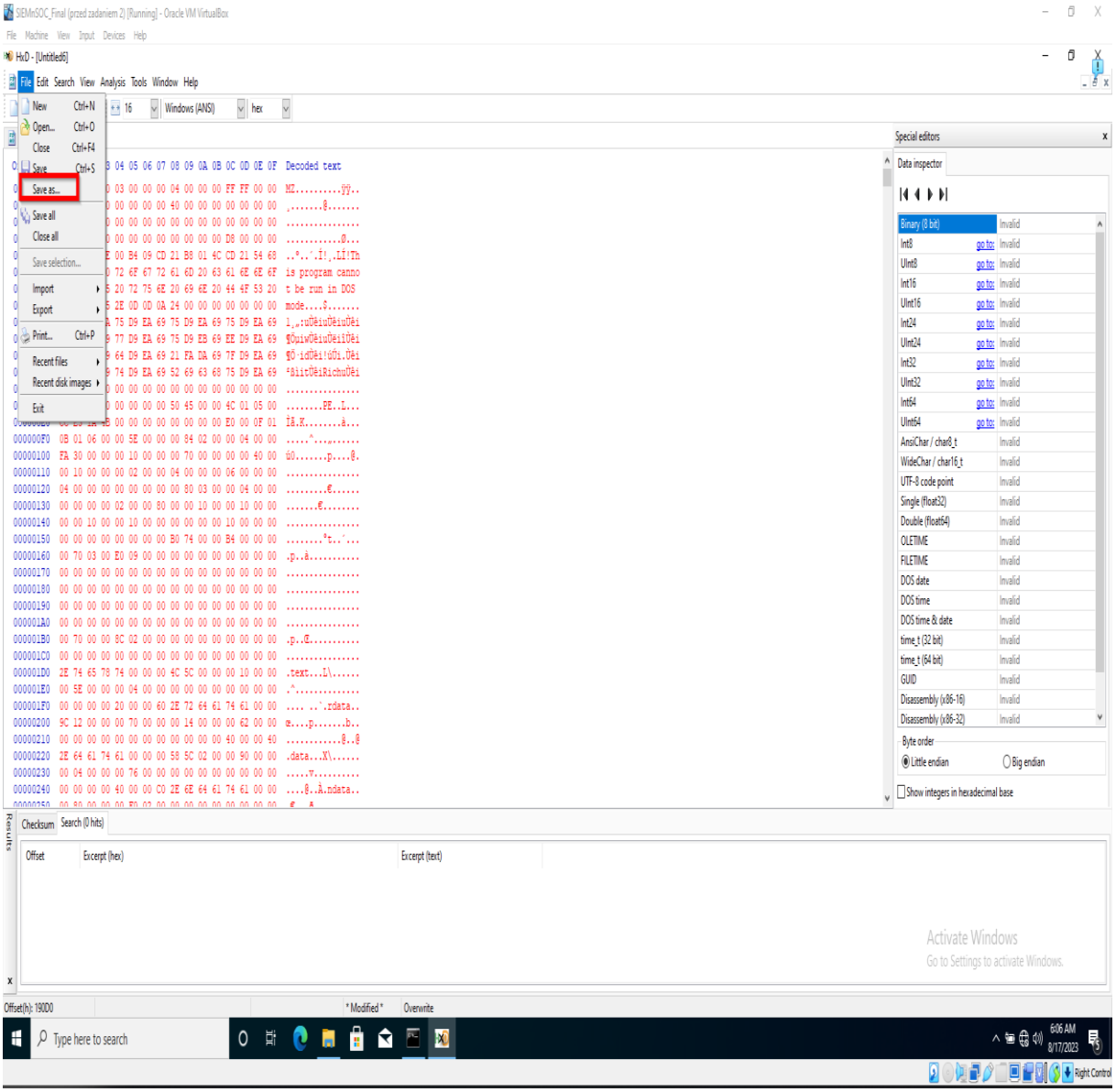
h)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HxD - [Untitled1]
File Edit Search View Analysis Tools Window Help
Windows (ANSI)
hex
Dog.jpg
Untitled1
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000
Undo Ctrl+Z
Cut Ctrl+X
Copy Ctrl+C
Paste insert Ctrl+V
Paste write Ctrl+B
Delete Del
Fill selection...
Select block... Ctrl+E
Select all Ctrl+A
Copy offset Alt+Ins
Special editors
Data inspector
Binary (8 bit) Invalid
Int8 go to: Invalid
UInt8 go to: Invalid
Int16 go to: Invalid
UInt16 go to: Invalid
Int24 go to: Invalid
UInt24 go to: Invalid
Int32 go to: Invalid
UInt32 go to: Invalid
Int64 go to: Invalid
UInt64 go to: Invalid
AnsiChar / char8_t Invalid
WideChar / char16_t Invalid
UTF-8 code point Invalid
Single (float32) Invalid
Double (float64) Invalid
OLETIME Invalid
FILETIME Invalid
DOS date Invalid
DOS time Invalid
DOS time & date Invalid
time_t (32 bit) Invalid
time_t (64 bit) Invalid
GUID Invalid
Disassembly (x86-16) Invalid
Disassembly (x86-32) Invalid
Byte order
Little endian
Big endian
Show integers in hexadecimal base
Results
Checksum
Search (0 hits)
Offset
Excerpt (hex)
Excerpt (text)
Activate Windows
Go to Settings to activate Windows.
Offset(h): 0
Overwrite
Type here to search
6:01 AM
8/17/2023
Right Control

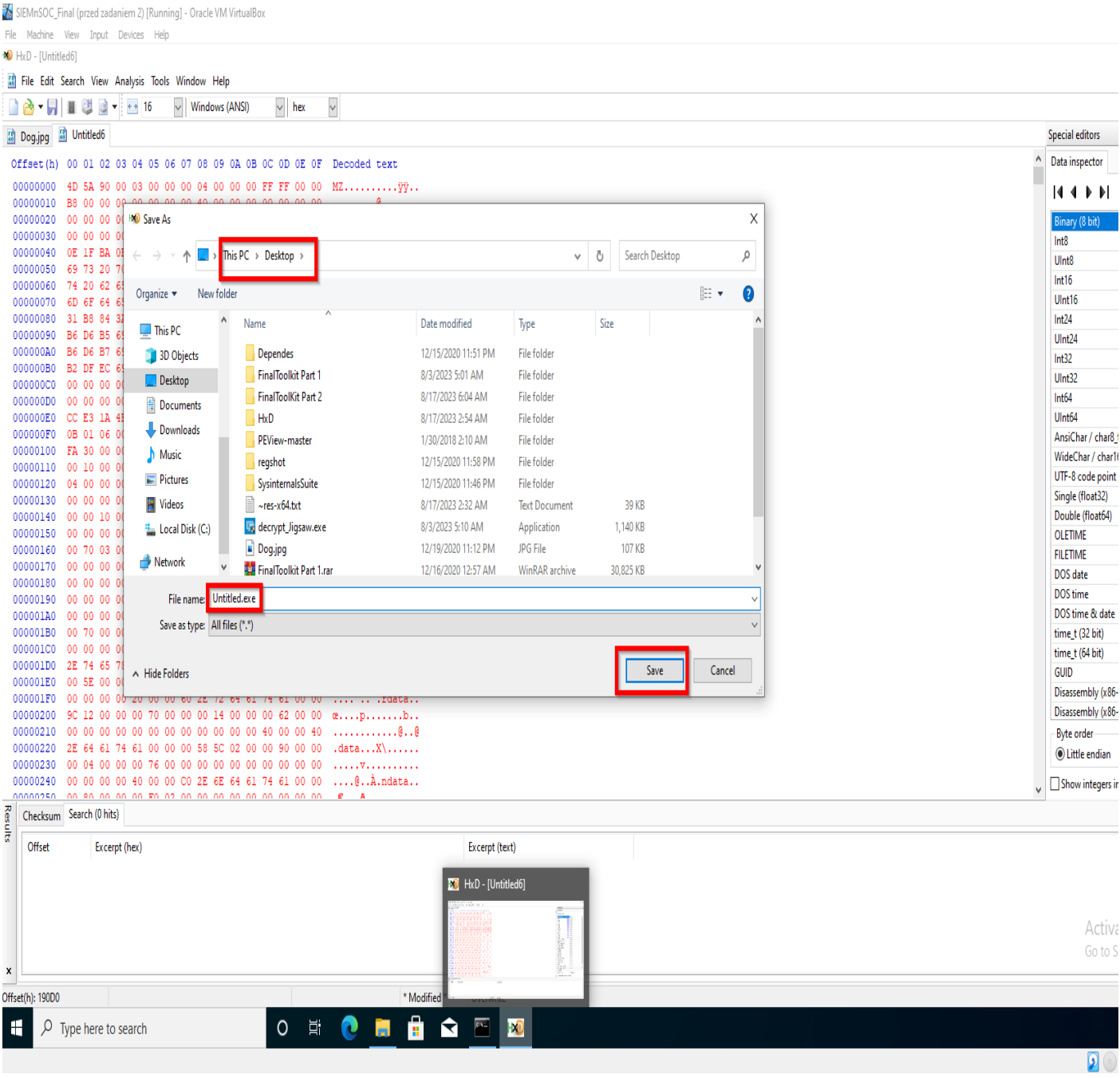
i)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HxD - [Untitled1]
File Edit Search View Analysis Tools Window Help
Windows (ANSI)
hex
Dog.jpg
Untitled1
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000
Confirm
This operation changes the file-size. Do you want to proceed?
Do not ask this question again
OK
Cancel
Special editors
Data inspector
Binary (8 bit)
Int8
UInt8
Int16
UInt16
Int24
UInt24
Int32
UInt32
Int64
UInt64
AnsiChar / char8_t
WideChar / char16_t
UTF-8 code point
Single (float32)
Double (float64)
OLETIME
FILETIME
DOS date
DOS time
DOS time & date
time_t (32 bit)
time_t (64 bit)
GUID
Disassembly (x86-16)
Disassembly (x86-32)
Byte order
Little endian
Big endian
Show integers in hexadecimal base
Results
Checksum
Search (0 hits)
Offset
Excerpt (hex)
Excerpt (text)
Activate Windows
Go to Settings to activate Windows.
Offset(h): 0
Overwrite
Type here to search
6:02 AM
8/17/2023
Right Control

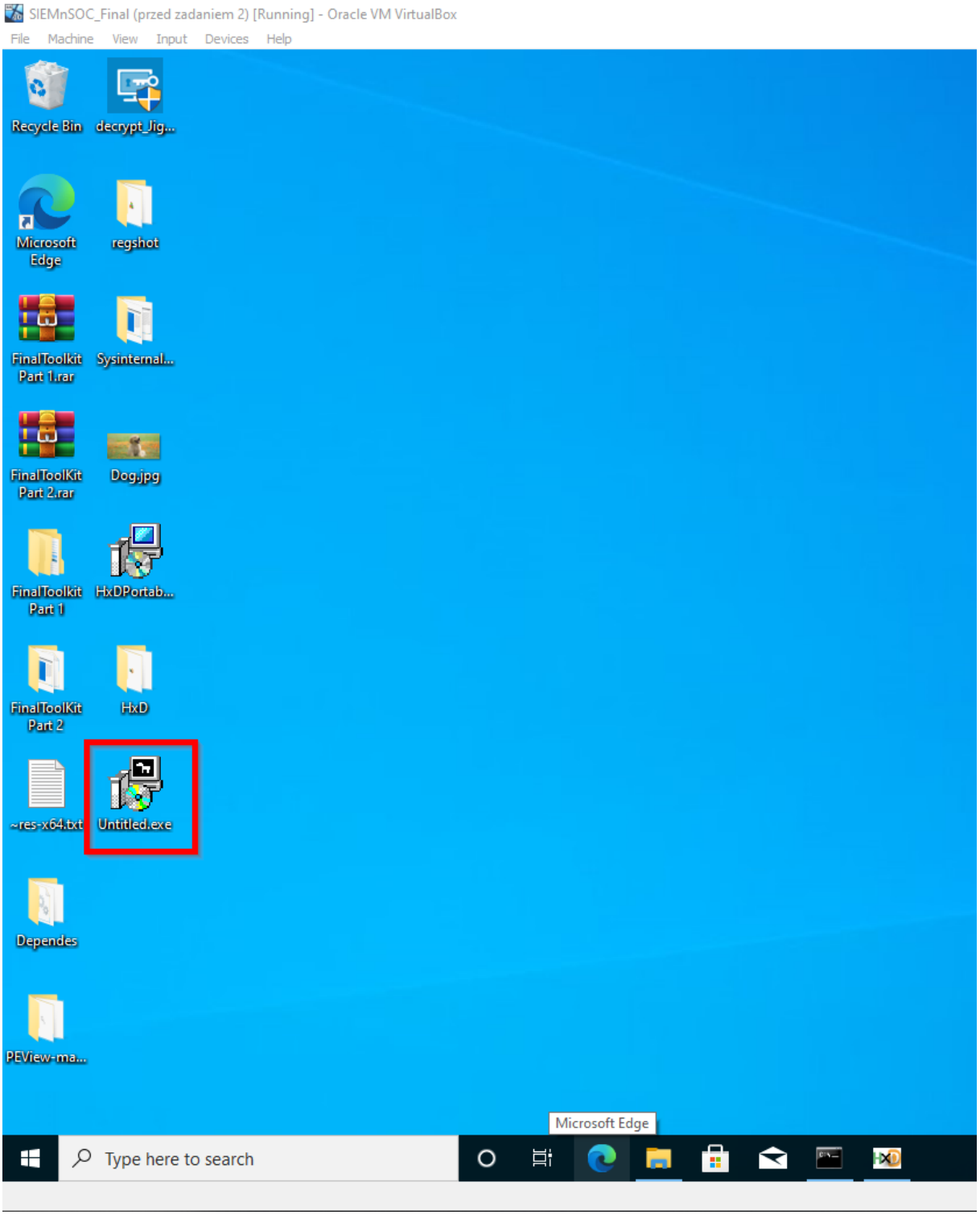
j)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
HxD - [Untitled6]
File Edit Search View Analysis Tools Window Help
New Ctrl+N
Open... Ctrl+O
Close Ctrl+F4
Save Ctrl+S
Save as...
Save all
Close all
Save selection...
Import
Export
Print... Ctrl+P
Recent files
Recent disk images
Exit
Special editors
Data inspector
Checksum
Search (0 hits)
Offset
Excerpt (hex)
Excerpt (text)
Activate Windows
Go to Settings to activate Windows.
Type here to search
6:06 AM
8/17/2023

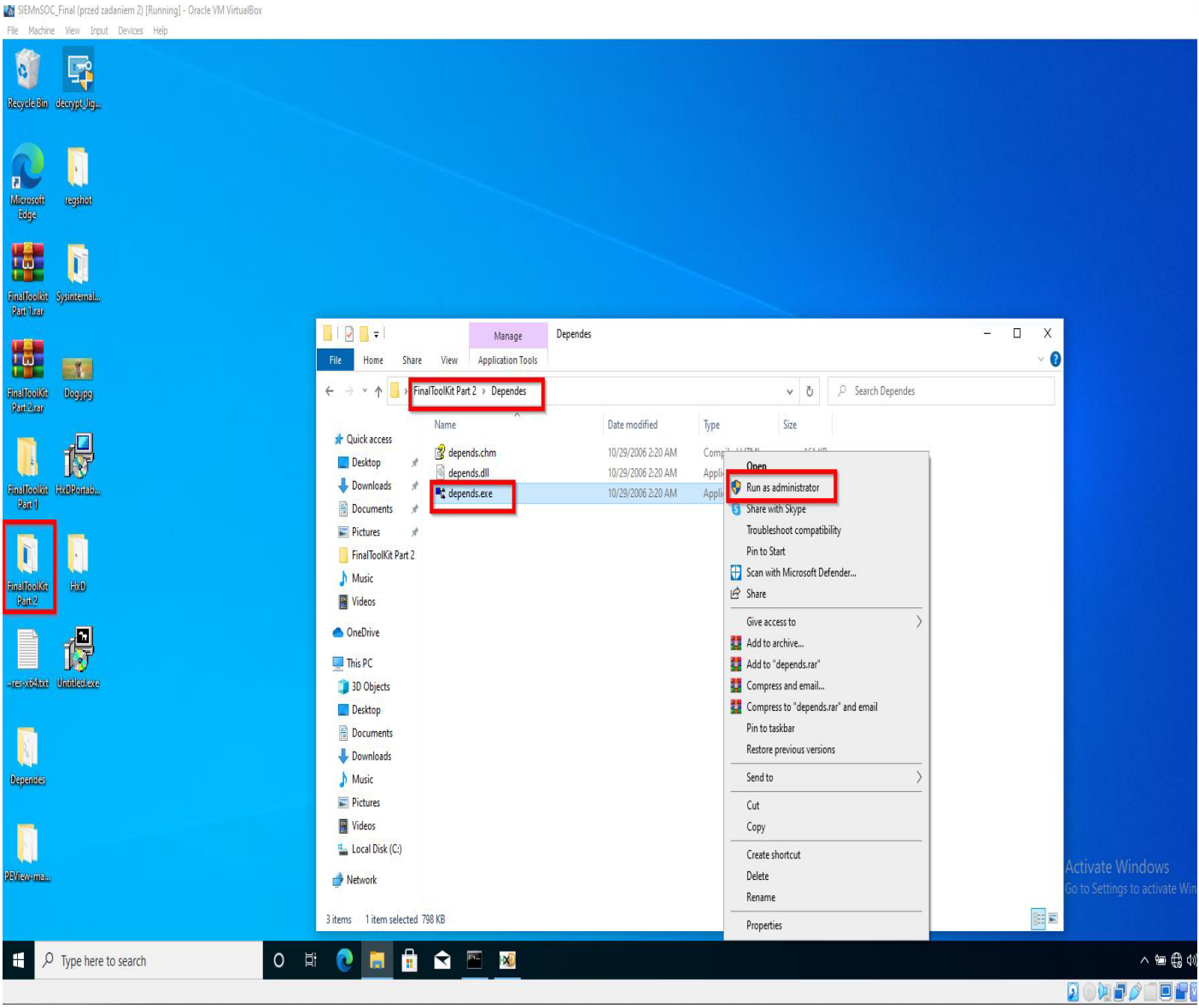
k)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HxD - [Untitled6]
File Edit Search View Analysis Tools Window Help
Windows (ANSI)
hex
Dog.jpg
Untitled6
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
Special editors
Data inspector
Save As
This PC › Desktop ›
Search Desktop
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name
Date modified
Type
Size
Dependes 12/15/2020 11:51 PM File folder
FinalToolkit Part 1 8/3/2023 5:01 AM File folder
FinalToolKit Part 2 8/17/2023 6:04 AM File folder
HxD 8/17/2023 2:54 AM File folder
PEView-master 1/30/2018 2:10 AM File folder
regshot 12/15/2020 11:58 PM File folder
SysinternalsSuite 12/15/2020 11:46 PM File folder
~res-x64.txt 8/17/2023 2:32 AM Text Document 39 KB
decrypt_Jigsaw.exe 8/3/2023 5:10 AM Application 1,140 KB
Dog.jpg 12/19/2020 11:12 PM JPG File 107 KB
FinalToolkit Part 1.rar 12/16/2020 12:57 AM WinRAR archive 30,825 KB
File name: Untitled.exe
Save as type: All files (*.*)
Hide Folders
Save
Cancel
Checksum
Search (0 hits)
Offset
Excerpt (hex)
Excerpt (text)
HxD - [Untitled6]
Offset(h): 190D0
* Modified
Type here to search

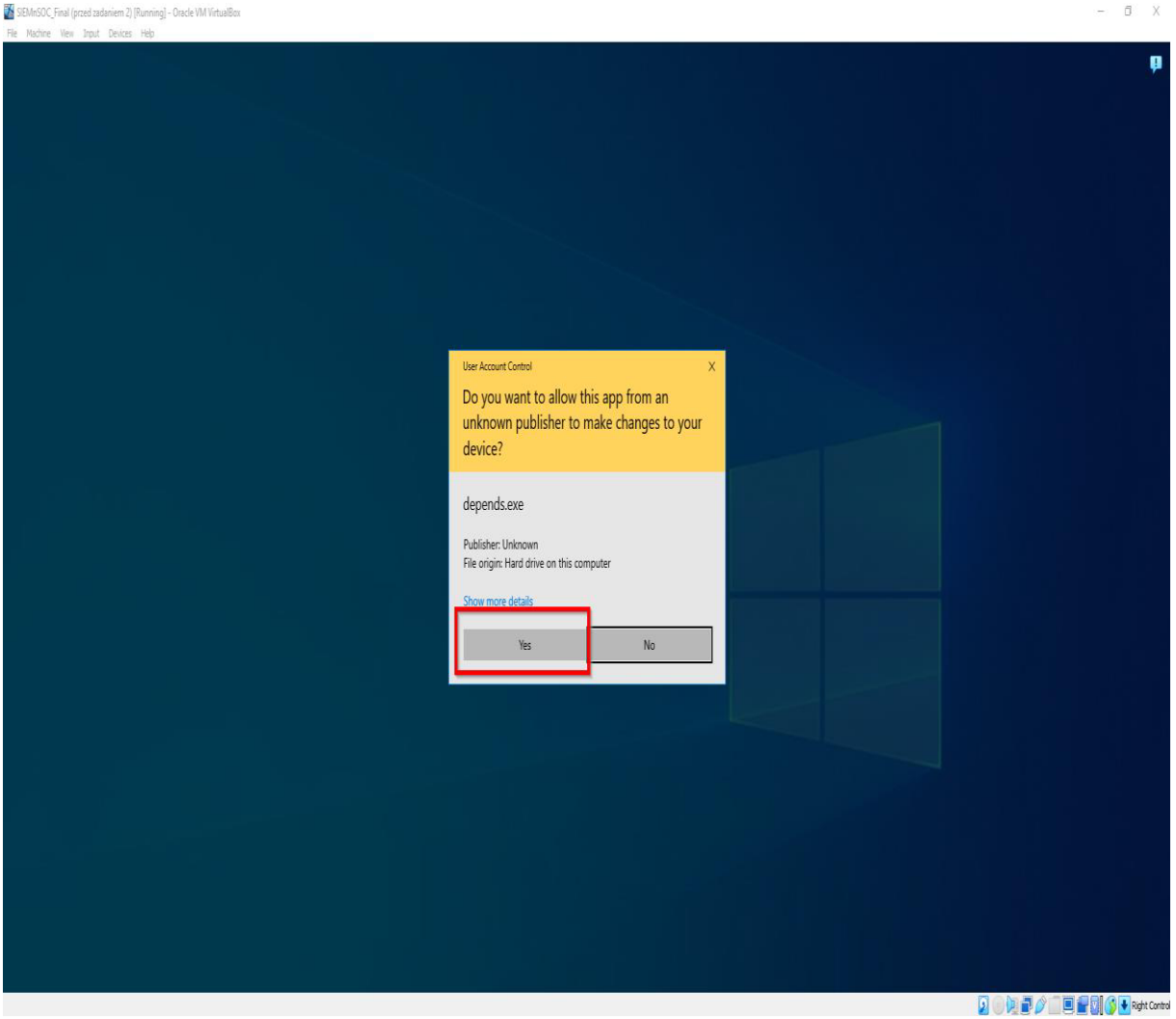
I)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
decrypt_lig...
Microsoft Edge
regshot
FinalToolkit Part 1.rar
Sysinternal...
FinalToolKit Part 2.rar
Dog.jpg
FinalToolkit Part 1
HxDPortab...
FinalToolKit Part 2
HxD
~res-x64.txt
Untitled.exe
Dependes
PEView-ma...
Microsoft Edge
Type here to search

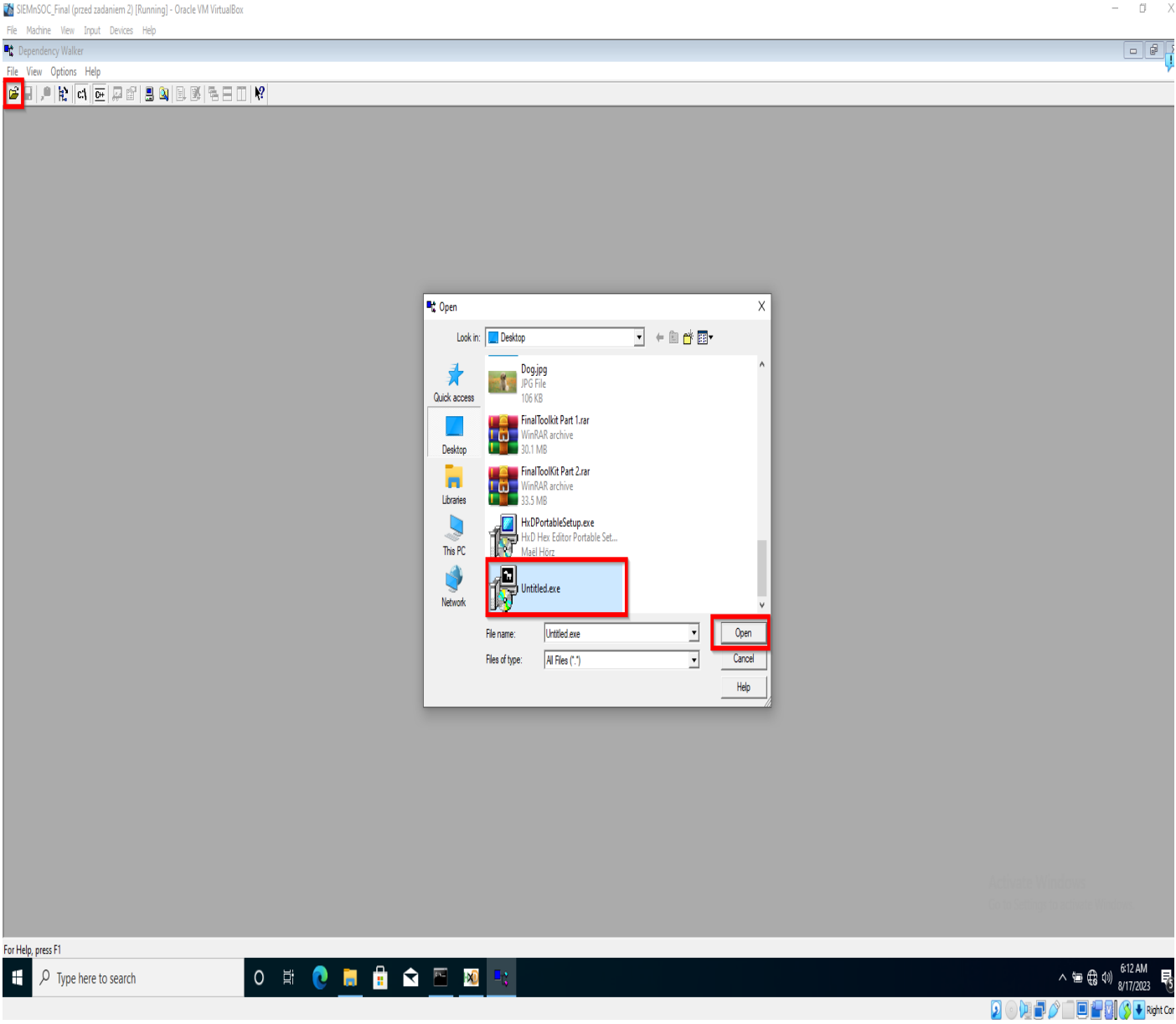
m)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
decrypt_jig...
Microsoft Edge
regshot
FinalToolkit Part 1.rar
Sysinternal...
FinalToolkit Part 2.rar
Dog.jpg
FinalToolkit Part 1
HxDPortab...
FinalToolkit Part 2
HxD
~res-x64.txt
Untitled.exe
Dependes
PEView-ma...
Manage
Dependes
File Home Share View Application Tools
FinalToolKit Part 2 › Dependes
Search Dependes
Name
Date modified
Type
Size
depends.chm 10/29/2006 2:20 AM
depends.dll 10/29/2006 2:20 AM
depends.exe 10/29/2006 2:20 AM
Quick access
Desktop
Downloads
Documents
Pictures
FinalToolKit Part 2
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
3 items 1 item selected 798 KB
Open
Run as administrator
Share with Skype
Troubleshoot compatibility
Pin to Start
Scan with Microsoft Defender...
Share
Give access to
Add to archive...
Add to "depends.rar"
Compress and email...
Compress to "depends.rar" and email
Pin to taskbar
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Activate Windows
Go to Settings to activate Win
Type here to search

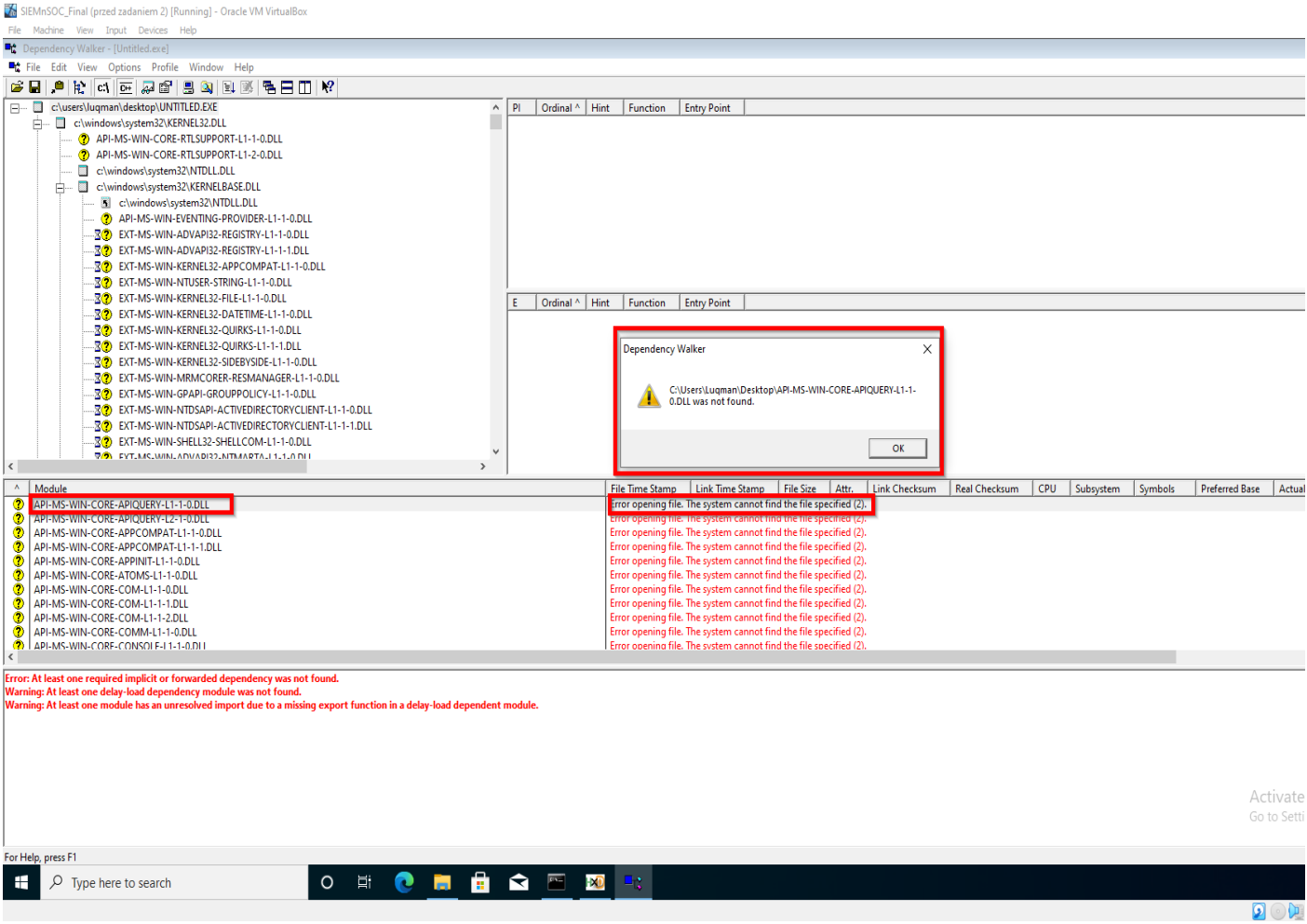
n)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
User Account Control
Do you want to allow this app from an unknown publisher to make changes to your device?
depends.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show more details
Yes
No
Right Control

o)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Dependency Walker
File View Options Help
Open
Look in: Desktop
Quick access
Desktop
Libraries
This PC
Network
Dog.jpg
JPG File
106 KB
FinalToolkit Part 1.rar
WinRAR archive
30.1 MB
FinalToolKit Part 2.rar
WinRAR archive
33.5 MB
HxDPortableSetup.exe
HxD Hex Editor Portable Set...
Maël Hörz
Untitled.exe
File name: Untitled.exe
Files of type: All Files (*.*)
Open
Cancel
Help
For Help, press F1
Type here to search
6:12 AM
8/17/2023

p)


SIEMnSOC_Final (przed zadaniem 2) [Running] - Oracle VM VirtualBox
Dependency Walker - [Untitled.exe]
c:\users\luqman\desktop\UNTITLED.EXE
c:\windows\system32\KERNEL32.DLL
API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
c:\windows\system32\NTDLL.DLL
c:\windows\system32\KERNELBASE.DLL
API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL
EXT-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL
EXT-MS-WIN-MRMCORER-RESMANAGER-L1-1-0.DLL
EXT-MS-WIN-GPAPI-GROUPPOLICY-L1-1-0.DLL
EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL
EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-1.DLL
EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL
PI Ordinal ^ Hint Function Entry Point
E Ordinal ^ Hint Function Entry Point
Dependency Walker
C:\Users\Luqman\Desktop\API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL was not found.
OK
Module
File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
Error opening file. The system cannot find the file specified (2).
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL
API-MS-WIN-CORE-APPINIT-L1-1-0.DLL
API-MS-WIN-CORE-ATOMS-L1-1-0.DLL
API-MS-WIN-CORE-COM-L1-1-0.DLL
API-MS-WIN-CORE-COM-L1-1-1.DLL
API-MS-WIN-CORE-COM-L1-1-2.DLL
API-MS-WIN-CORE-COMM-L1-1-0.DLL
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
For Help, press F1
Type here to search